Report of the
Defense Science Board
2008 Summer Study on

Capability Surprise

Volume I: Main Report

September 2009

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **SEP 2009**	2. REPORT TYPE	3. DATES COVERED **00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE **Report of the Defense Science Board 2008 Summer Study on Capability Surprise Volume 1: Main Report**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Under Secretary of Defense,For Acquisition, Technology, and Logistics,Washington,DC,20301-3140**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**103**	

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense. The 2008 Summer Study on Capability Surprise completed its information-gathering in August 2008.

This report is unclassified and cleared for public release.

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR: Under Secretary of Defense for Acquisition, Technology
and Logistics

SUBJECT: Final Report of the Defense Science Board 2008 Summer Study on
Capability Surprise

I am pleased to forward the final report of the Defense Science Board 2008 Summer Study on Capability Surprise. This report offers important considerations for the Department of Defense in response to future threats to our nation's security.

This study concerns itself with the matter of capability surprise, which can arise from many sources—scientific breakthrough, rapid fielding, operational innovation. It considers two fundamental kinds of surprises: 1) those specific few, that because of their unique characteristics and impact, the nation should be anticipating—referred to as "known surprises"; and 2) those that arise unexpectedly out of a myriad of other possibilities, seemingly without warning—the "surprising surprises." The premise of the study is that surprise cannot be eliminated, but it can—and must—be managed.

Today, the Department of Defense and the nation are not adequately prepared to manage surprise—to reduce the potential for its occurrence or to respond rapidly and appropriately, should it occur. Thus, the study's recommendations focus on improving critical processes and implementing new ones: scanning and assessment, red teaming and exercising, rapid fielding, strategic intelligence, and integration and management.

I endorse all of the study's recommendations and encourage you to forward the report to the Secretary of Defense.

Paul G. Kaminski

Dr. Paul G. Kaminski
Chairman

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE BOARD

MEMORANDUM FOR: Chairman, Defense Science Board

SUBJECT: Final Report of the Defense Science Board 2008 Summer Study on Capability Surprise

The instability and cultural complexities in today's world, the breadth of security challenges, and the capability not only of states, but of non-states and extremists to "make really bad things happen" create an environment in which the potential for surprise has reached new levels. As of yet the nation has found no simple form of deterrence to deal with this complex environment. Thus, we as a nation must be prepared to deal with surprise in new ways.

This study addresses the issue of capability surprise—what it is, why it happens, what can be done to reduce the potential for its occurrence, and how the Department of Defense and the nation can be better prepared to respond appropriately.

Capability surprise can spring from many sources: scientific breakthrough in the laboratory, rapid fielding of a known technology, or new operational use of an existing capability or technology. A review of many surprises that occurred over the past century suggests that surprises tend to fall into two major categories:

- "Known" surprises—those few that the United States should have known were coming, but for which it did not adequately prepare. For this category of surprise, the potential and evidence are clear; the effects are potentially catastrophic; and dealing with them is difficult, costly, and sometimes counter-cultural. We specifically include space, cyber, and nuclear in this category today. We might also have included bio, but with a focus on threats to military operations, we chose not to.
- "Surprising" surprises—those many that the nation might have known about or at least anticipated, but which were buried among hundreds or thousands of other possibilities. In this case, the evidence and consequences are less clear, the possibilities are many, and the nation cannot afford to pursue them all.

In both cases, the biggest issue is not a failure to envision events that may be surprising. It is a failure to decide which ones to act upon, and to what degree. That failure results, at least partially, from the fact that there is no systematic mechanism in place within DOD or the interagency to help decide which events to act on aggressively, which to treat to a lesser degree, and which to ignore, at least for the time being. Thus, the principle recommendations of this study focus on developing the approaches and the talent to better manage surprise—to prevent it from happening or, should surprise occur, to be in a position to rapidly mitigate its consequences.

The Department must take several important steps in order to more effectively manage capability surprise:

1. Integration and management of surprise at a high enough level to affect senior decision making. Secretary of Defense formally establish a Capability, Assessment, Warning and Response Office (CAWRO) to provide DOD senior

leadership with timely assessment and warning of potentially high-risk adversary capabilities with options and recommendations for addressing them.

2. Red teaming as the norm instead of the exception. Secretary of Defense direct the use of red teaming throughout DOD by developing and employing best practice guides, intellectual focus in professional military education, and more aggressive use of red teams in exercises. The Secretary should also lead by example and establish a strategic-level red team to challenge and inform national security and top level defense policies and strategies.

3. Rapid fielding that is truly rapid and can be effectively employed when the circumstances warrant. The Under Secretary of Defense for Acquisition, Technology, and Logistics establish a standing Rapid Capability Fielding Office (RCFO) to improve DOD capabilities for addressing priority surprise capability gaps and supporting urgent war fighter needs.

4. Pointed improvements in “strategic” intelligence. The Director, National Intelligence Warning Office, in the National Intelligence Council, provide adequate resources for “strategic intelligence” and establish a cell within the CAWRO. The cell and its interaction with the CAWRO support multiple objectives —to better monitor adversary intent and capabilities over time, to help focus collection efforts on key activity signatures, and to continuously update key adversary vulnerabilities that the nation can exploit. Improvements are also needed in the area of detecting foreign denial and deception.

5. For known surprises, the Secretary of Defense establish a formal mechanism to ensure Department progress in addressing the limited number of most critical threats. Focus is needed on ongoing assessments; operational exercises, games, and red teaming; and improving the nation’s abilities to deter, detect, prevent, mitigate, fight through, and use appropriate offensive measures.

For surprise management to be successful, however, there needs to be support from leadership at the highest levels—a recurring theme of this study. Emphasis should be placed on encouraging alternative viewpoints, requiring broad risk/opportunity assessment, integrating and synthesizing, and enhancing knowledge through cross-domain teaming. Without such leadership, the tendency will be to maintain the status quo … and the nation will be seriously surprised.

Dr. Miriam John	Mr. Robert Stein
Co-Chair	Co-Chair

Table of Contents

Executive Summary

This study addresses the issue of capability surprise—what it is, why it happens, what can be done to reduce the potential for its occurrence, and how to better prepare the Department of Defense (DOD) and the nation to respond appropriately.

Nature of Surprise

Why should the Department be especially worried about surprise now? First, technology and globalization have empowered first- and second-tier states, non-states, and even individual extremists alike. Having the ability to "make really bad things happen" is no longer the sole province of a few major states. Moreover, moral or ethical norms by which the United States operates may be irrelevant to many potential adversaries. Second, growing social, cultural, religious, economic, and technical interdependencies have made it more difficult to predict national and regional unrest. There is greater instability in the world and the potential for unintended consequences is much higher. Finally, a key difference in the world today is reflected in the breadth of security challenges, the understanding of which demands deeper and more timely knowledge than the nation's intelligence, diplomatic, and investment capacities can provide.

As yet, there is no simple form of deterrence equivalent to that which worked so effectively during the Cold War. Thus, the potential for serious surprise has reached new levels and we as a nation must be prepared to deal with it in new ways.

While the potential effects of surprise have increased, the types of surprise that exist and the reasons that surprise occurs are neither new nor peculiar to the current era. One of the most prevalent reasons for surprise is a failure to look at the world from time to time with fresh eyes—to question basic assumptions. Instead, it is human nature to stay mired in familiar, existing, "comfortable" paradigms. When those paradigms change, or conventional wisdom turns out to be wrong, the nation gets surprised.

Surprise can spring from many sources. It can arise in the laboratory—a result of scientific breakthrough. It can arise during the transition from concept to fielded product: rapid fielding of the same technology can create tremendous advantage to whoever fields the system first. It can also arise when an existing capability is employed in an unconventional way or when low-end technology is adapted in unforeseen ways that create an effective capability against high-end U.S. systems.

A review of many surprises that occurred over the past century suggests that surprises tend to fall into two major categories, around which this study is organized:

- "Known" surprises are those the United States should have known were coming, but for which it did not adequately prepare. For this category of surprise, the potential and evidence are clear; the effects are potentially catastrophic; and dealing with them is difficult, costly, and sometimes counter-cultural. They are, in effect, a "shame on us" if they occur.
- "Surprising" surprises are those the nation might have known about or at least anticipated, but which were buried among hundreds or thousands of other possibilities. In this case, the evidence and consequences are less clear, the possibilities are many, and the nation cannot afford to pursue them all.

In both cases, the biggest issue is not a failure to envision events that may be surprising; it is a failure to decide which ones to act upon, and to what degree. That failure results, at least partially, from the fact that there is no systematic mechanism in place within DOD or the interagency to help decide which events to act on aggressively, which to treat to a lesser degree, and which to ignore, at least for the time being.

"Known Surprises"

This study identified three "known surprises": cyber surprise, surprise in space, and nuclear surprise. All three have the potential to create serious damage to both the military and civil sectors. All three, particularly in recent years, are becoming easier to execute because the knowledge to do so is more pervasive and/or the technology or critical components are more readily available—either because materials can be adapted from civilian use and are therefore difficult to detect, or because weapons proliferation is not being effectively controlled. All three show indications of spreading as more potential adversaries are attaining capabilities. Conversely, none of the three, in numerous threatening scenarios, can be easily or definitively attributed, and therefore, will be difficult to deter by the threat of retaliation.

Perhaps most worrisome, all three—cyber, space and nuclear—are characterized by lack of adequate preparation on the part of the United States.

Cyber Surprise

Over the past several years, DOD has become increasingly "net-centric." This entails networking many different sources of sensor and informational data with multiple processing nodes and geographically distributed users to achieve unprecedented levels of situational awareness, data distribution, and operational coordination. Net-centric operations bring both an increase in capability as well as increased dependence on the viability of the network. Thus, new vulnerabilities are created. Because information technology is ubiquitous in almost all war fighting capabilities, networks can reasonably be viewed by the adversary as the "center of gravity" for disrupting U.S. military capabilities. In essence, networks have become a combat capability and need to be defended as such.

RECOMMENDATIONS: CYBER SURPRISE

Chairman, Joint Chiefs of Staff, direct action on a series of exercise activities to gain operational understanding of the impact of cyber attacks:

- What and how deep are U.S. vulnerabilities?
- How do they impact the nation's ability to fight?
- How can the military fight through?

Vice Chairman, Joint Chiefs of Staff, direct the Services and combatant commands to initiate a series of activities to increase the resistance of critical information systems to cyber attack.

Iterate the two activities above to inform understanding of vulnerabilities, efficacy of corrective measures, and new measures that need to be taken.

Surprise in Space

As with cyber, the effective use of space is of critical importance to the United States. Yet vital assets exhibit increased vulnerabilities. The nation relies on space-based capabilities not only to meet the needs of joint military operations worldwide, but also to support diplomatic, informational, and economic efforts. Space is essential to strategic and tactical military communications; missile warning; intelligence; and position, navigation, and timing. Nevertheless, techniques to deny the use of space are proliferating. Thus, space can no longer be considered the “safe haven” or sanctuary of the past. Instead, the United States should view space as a potential combat zone, where space assets can be attacked physically or electronically. In response, the national policy should drive development of both defensive and counter-space capabilities, consistent with U.S. treaty obligations.

RECOMMENDATIONS: SURPRISE IN SPACE

Chairman, Joint Chiefs of Staff, direct combatant commanders and military service chiefs to understand the operational impact of a degraded space environment and develop tactics, techniques, and procedures to fight through.

- U.S. Joint Forces Command should factor into joint/combined war games and appropriate exercises

U.S. Strategic Command develop foundational requirements to increase the robustness of the military space architecture across appropriate areas of awareness, assessment, protection, survivability, reconstitution, and fall backs.

Nuclear Surprise

The nation has been ignoring for some time the warning signs that, with respect to nuclear weapons, the “peace dividend” from the end of the Cold War is wearing increasingly thin. All declared nuclear powers, with the exception of the United States, are modernizing their nuclear forces and some currently non-nuclear states are working to acquire a capability of their own. Interest on the part of non-state groups in acquiring nuclear weapons has added to these concerns. In addition, of considerable concern are the rhetoric and actions of Russia and China. They both maintain a declaratory policy that they would be willing to use tactical nuclear weapons if necessary to stop an aggressor with superior conventional capabilities. Yet in the face of these external trends and actions, many prominent leaders in the United States still hold fast to the belief that no one would dare to use nuclear weapons against our nation. The belief is accompanied by a lack of investment in force modernization.

RECOMMENDATIONS: NUCLEAR SURPRISE

The administration should reestablish a focus on nuclear issues as a top priority in national security policy and strategy. It must:

- Develop a comprehensive strategy analogous to what evolved during the Cold War, but relevant to 21st century multi-lateral issues.
- Actively engage Congress to develop a bipartisan consensus.

The Secretary of Defense should direct that implementation of the next Nuclear Posture Review be given priority by senior military and civilian leadership:

- Establish needs, programming strategies, and resources for modernizing critical force elements (Office of the Secretary of Defense, Air Force, Navy).
- Direct that critical war fighting and support functions be assessed for nuclear survivability, and that measures be taken to ensure mission success in the wake of a nuclear attack (Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)); Vice Chairman, Joint Chiefs of Staff).
- Reestablish valued career tracks for nuclear expertise (military services).
- Re-introduce nuclear issues into education, training, gaming, and exercises (combatant commanders, military services).

Overarching

The Secretary of Defense must take the lead in addressing known surprises—to deal with these threats before they actually do become surprises.

OVERARCHING RECOMMENDATIONS: KNOWN SURPRISES

The Secretary of Defense establish a formal mechanism to ensure Department progress in addressing the limited number of most critical threats—the known surprises. The Secretary direct:

- An ongoing assessment of the risks posed by these known surprises: foreign capabilities, U.S. strengths and vulnerabilities, and net potential consequences

- Services and appropriate combatant commands to perform a series of operational exercises, games, and red teaming activities that both inform and reflect the risk assessment activity above
- USD (AT&L) and Chairman, Joint Chiefs of Staff, identify a series of measurable goals and time frames for improving the nation's abilities to deter; fight through; detect, prevent, and mitigate; and use appropriate offensive measures

The Secretary of Defense and Chairman, Joint Chiefs of Staff, engage and educate congressional leadership on these issues.

Surprising Surprises

Rarely is there a case of true surprise. Post mortems almost always identify that someone had provided warning, but that the warning was not heeded. The reasons can be many, but most often, before a particular surprise presents itself, it is typically obscured by many other, equally plausible—or implausible—possibilities, none of which stand out from the rest. Given that the nation cannot afford to address every possible "surprise," the question addressed by this study was whether an approach could be defined that would allow the nation to systematically decide which potential surprise(s) should be addressed and how.

Managing Surprise

The study team explored organizations that seemingly manage surprise well. A comparison of the practices of these various organizations to those in the Department of Defense showed that the Department does in fact have some of the elements that might contribute to effective surprise management. Yet, many key ingredients are also lacking. In addition, even if all of the individual elements existed, there is currently no effective means for integrating among them. In other words, the Department lacks a process for managing surprise.

The study identified five steps that, integrated together, constitute a robust approach to managing surprise:

- A scanning and sifting process that narrows the many possibilities to the most worrisome few
- A "red" capability projection function that takes a "deeper dive" on the worrisome few through analysis, simulation, experimentation, and/or prototyping

- A net assessment process in which the deeper understanding of "red," gained through capability projection, is played against blue capabilities in order to assess the degree to which the nation can address the threat or adapt capabilities already in hand
- An options analysis team to provide an unbiased evaluation—or "rack and stack"—of the alternatives should blue capabilities prove inadequate
- An ability to produce a decision package that can be acted upon by senior leadership

Essential also is an integration function that links the steps together and then iterates continuously in order to account for new knowledge and the dynamic set of adversaries that the nation faces. Surprise can be managed—not to prevent it from occurring, because that is not a realizable objective—but rather to hedge against higher risk possibilities and, equally important, to create the agile mechanisms that should allow more timely response should the unexpected occur.

Redressing Shortcomings

The Department must take several important steps in order to more effectively manage capability surprise:

- Integration and management of surprise at a high enough level to affect senior decision making
- Red teaming as the norm instead of the exception
- Rapid fielding that is truly rapid and can be effectively employed
- Pointed improvements in "strategic" intelligence

Addressing each of these areas individually is difficult enough, much less as a set. But planning under uncertainty has become the norm, which in turn calls for new and/or different approaches and institutional processes.

Integration and Management. The elements of surprise management are unlikely to achieve their potential impact, even if perfected, without some function that integrates and guides them. The Defense Science Board is normally reluctant to recommend creating new organizations, but in this case, the Board feels that it is critical to the success of managing surprise.

RECOMMENDATION: INTEGRATION AND MANAGEMENT

The Secretary of Defense formally establish a Capability Assessment, Warning, and Response Office (CAWRO) to provide DOD senior leadership with timely assessment and warning of potentially high-risk adversary capabilities, with options for addressing them.

Establishing the CAWRO has the added advantage of providing the "go-to" organization for undertaking the ongoing assessment recommended above for known surprises.

Red Teaming. Red teaming has been recommended for many years in numerous ways, but has yet to become a cultural norm for DOD—especially in addressing strategic-level issues or as a part of major acquisitions or exercises. We focus here on recommendations that address the critical role of red teaming for successful surprise management, but red teaming is important in its own right. Regardless of the motivation, red teaming will not become pervasive and persistent without sustained and aggressive leadership from the top. We recommend the following steps.

RECOMMENDATIONS: RED TEAMING

The Secretary of Defense direct the use of red teaming throughout DOD:

- All organizations develop and maintain red teaming best practice guides.
- Make red teaming the subject of continuing intellectual activity and professional military education and other relevant institutions.
- Require, with the Chairman, Joint Chiefs of Staff, more aggressive use of red teams in exercises and ensure retention and application of lessons learned.

The Secretary lead by example and establish a strategic-level red team to challenge and inform national security and top level defense policies and strategies

The Office of the Secretary of Defense, combatant commands, and military services tie red-teaming products to all elements of surprise management.

Rapid Fielding. The normal practice of establishing *ad hoc* organizations in response to individual urgent war fighter needs or pop-up surprises will not result in an effective capability within the Department. It appears that the

Department recognizes the need to “clean up the mess” of the many existing organizations and is taking steps to create a more robust innovation process. The success of any changes, however, depends on the discipline of leadership to create effective project teams for the task at hand and then dissolve those teams once their mission is performed. This study considered a number of options and offers the following recommendation.

RECOMMENDATION: RAPID FIELDING

The USD (AT&L) establish a standing Rapid Capability Fielding Office (RCFO) to improve DOD capabilities for addressing priority surprise capability gaps and supporting urgent war fighter needs. The office should:

- Report directly to the USD (AT&L)
- Operate on colorless money
- Consolidate most, if not all, existing OSD rapid fielding initiatives into one organization, except for Joint Improvised Explosive Device Defeat Organization (JIEDDO)
- Form dedicated expert project teams, with predefined sunset; each individual team:
  - implements a single, time-critical, priority acquisition and/or fielding project
  - is staffed with a small number of exceptional can-do people
  - has goals focused on solving a specific challenge
  - derives support from mainstream organizations as needed
  - up front plans for and negotiates transition of all ongoing efforts to lead Service with longer term responsibility
- Provide permanent core of enabling services

Strategic Intelligence. Whether all or part of the recommendations of this study is acted upon, two important functions of the intelligence community must be strengthened in order to support any aspect of surprise management. One is to greatly improve “strategic” intelligence that monitors adversary intent and capabilities over time and continuously updates key adversary vulnerabilities that the nation can exploit. The second is in the area of detecting foreign denial and deception—which effectively constitutes red teaming within the intelligence community.

RECOMMENDATIONS: STRATEGIC INTELLIGENCE

The DNI Warning Office, in the National Intelligence Council, provide adequate resources for “strategic intelligence” and establish a cell within the CAWRO.

The Under Secretary of Defense for Intelligence establish teams in the intelligence community and Department of Defense especially to support the CAWRO, to focus on detection of adversary denial and deception.

The Essential Requirement of Leadership

A recurring theme of this study is the critical need for leadership at the highest levels of the Department if the nation is going to be successful in anticipating, preparing for, rapidly countering, mitigating the effects of, and rebounding from strategic and/or existential surprise. Emphasis should be placed on:

- Encouraging alternative viewpoints, some of which challenge the status quo
- Requiring broad risk/opportunity assessment across a wide range of alternatives
- Integrating and synthesizing from a range of inputs and approaches—from “lessons learned” to innovation
- Enhancing knowledge through cross-domain teaming with shared accountabilities and recognition

Without this type of leadership, the essential steps of surprise management—that will question strategies, objectives, and methods and recommend different ways of doing things, particularly at the strategic level—will be unable to overcome the natural tendency of large organizations to maintain the status quo...and the nation will be seriously surprised.

Chapter 1. The Nature of Surprise

This study, conducted by the Defense Science Board (DSB), addresses the issue of capability surprise—what it is, why it happens, what can be done to reduce the potential for its occurrence, and how to better prepare the Department of Defense (DOD) and the nation to respond appropriately.

But why should DOD worry about surprise now? Hasn't it always been an issue? At the tactical level, yes. Troops expect it, prepare and train for it, adapt procedures to mitigate its effects, and employ surprise in their operations as a standard tactic against adversaries. But at the strategic and existential levels, there is a new concern regarding surprise. In prior years, only a major nation state had the potential to surprise the United States in ways that threatened its very existence or that could seriously change the American way of life. The former Soviet Union was such a nation state during the Cold War and had highly valued assets, both military and civilian, that could be held at risk. Although there were clearly differences, in many ways both nations shared understandable value structures and thus were amenable to deterrence. The United States adopted a clear and easily understood strategy for deterrence. The nation went to great lengths and expended vast resources to ensure that its deterrent posture and technical leadership always remained viable.

Today, however, with globalization of technology and proliferation of weapons of mass destruction (WMD), it is possible for just a handful of individuals to do harm to the U.S. society and its military on a scale comparable to nation states—given the right tools and widely-available knowledge. And unlike the case with nation states, clear attribution may be much more difficult. As yet, there is no simple form of deterrence equivalent to that which worked so effectively during the Cold War. Thus, the potential for serious surprise has reached new levels and we as a nation must be prepared to deal with it in new ways.

There are other issues as well. Despite significant U.S. science and technology prowess, numerous paths exist for adversaries to develop capabilities that do not rely on leading-edge science. These capabilities can sometimes be achieved at a significant cost advantage over U.S. capabilities. And while they generally pose a tactical threat, some can have effects that rise to strategic levels. No better recent example can be found than the effective use and rapid adaptation of improvised explosive devices (IEDs) by adversaries in Iraq. Such trends will only be exacerbated by the accessibility of weapons technology and systems on the international market.

Capability development paths that do not use cutting edge science and technology also exist for the United States, and may create opportunities for the nation to reverse the situation and employ cost-imposing strategies on adversaries. Our nature, however, has not been to pursue such avenues. Yet even if those opportunities are pursued, the nation is still likely to be surprised since the avenues for surprise are so numerous. Thus, for all of the reasons highlighted above, it is in the nation's interest to better understand the nature of surprise—what types of surprises may arise and why—and to best position itself to prevent or mitigate capability surprise in the future.

A Historical Perspective

Surprise is not a new phenomenon and can spring from many sources. It can arise in the laboratory—a result of scientific breakthrough. It can arise during the transition from concept to fielded product: rapid fielding of the same technology can create tremendous advantage to whoever fields the system first. It can also arise when an existing capability is employed in an unconventional way or when low-end technology is adapted in unforeseen ways that create an effective capability against high-end U.S. systems.

While the potential effects of surprise have increased, the types of surprise that exist and the reasons that surprise occurs are neither new nor peculiar to the current era. One of the most prevalent reasons for surprise is a failure to look at the world from time to time with fresh eyes—to question basic assumptions. Instead it is human nature to stay mired in familiar, existing, "comfortable" paradigms. When those paradigms change, or conventional wisdom turns out to be wrong, the nation gets surprised.

History is replete with examples of surprise. An interesting one, that looks back more than 100 years, involves the Wright brothers and the question of whether air flight would ever be possible. On October 9, 1903, the *New York Times* published a learned article extolling the near impossibility of creating a heavier-than-air flying machine. The author's prognosis was that "The flying machine which will really fly might be evolved by the combined and continuous efforts of mathematicians and mechanicians in from one million to ten million years." That very same day, Orville Wright's diary entry read "We started assembly today" of the Kitty Hawk flying machine. A revolutionary surprise was in the making.

Then, as now, leaning too heavily on conventional wisdom often "gets it wrong" and leads to surprises that could otherwise have been avoided.

A review of many surprises that occurred over the past century, suggests that surprises tend to fall into two major categories. *One category is comprised of surprises that appear to come from nowhere.* They emerge because observable activities that might have held clues are buried among literally hundreds of other activities, with little to distinguish among them, so there is little or no warning. Even when someone postulates the potential surprise, there is little to distinguish it from the myriad of other surprise possibilities.

The second category contains surprises for which there are some more obvious warning signs. In this second category the evidence of a potential event is less ambiguous, the potential for damage more significant, yet there is little or no preparation to prevent or mitigate the circumstances. The lack of preparedness is often due to a failure to act, or a long delay in decision-making, in spite of the evidence, either because of political, institutional, or economic obstacles.

An example of the latter category occurred during the rise of Nazi Germany prior to World War II. In 1939, based on information received from colleagues inside Germany and the United States, Albert Einstein was asked to use his influence to urge President Roosevelt to begin a program in response to Germany's ongoing development of the atomic bomb. Einstein's letter to Roosevelt spelled out the realistic possibility of an atomic bomb being developed, of the need to worry about Germany as a potential adversary, and the strategic consequences that could result if Germany were successful. Roosevelt's initial response was a familiar one—to "study" the problem, investing $6,000 annually to do so.

Two years later, increasingly alarmed at the possibility of Germany obtaining the atomic bomb with no viable U.S. response, Einstein wrote a second letter—motivated in part by the urging of other world-renowned physicists Edward Teller, Leo Szillard, and Eugene Wigner. This time, Roosevelt responded more aggressively and initiated what later became known as the Manhattan Project. While the United States was ultimately successful in developing its own atomic bomb, two years had been lost because Roosevelt failed to act decisively when initially presented with evidence that top German scientists were working on a device and, if they were successful, the potential for disaster was unprecedented.

One of the first efforts undertaken during the course of this summer study was to examine situations that "surprised" the United States over the past half century (Table 1). This investigation resulted in one clear finding: rarely has the United

States been surprised because no one anticipated the situation. In nearly every case, the event had been foreseen by someone, somewhere. But in nearly every case, other than those in which the nation chose to take a conscious risk, the forecast of some future event was overlooked because either it did not stand out among hundreds of others that seemed to have more or less the same validity, or the circumstances were such that it was easier to ignore the risk than to act upon it. No mechanism existed to help guide decision-makers in identifying which potential events to prepare for, and which to ignore and accept risk. The study team's conclusion was that the problem has rarely been "surprise"—it has generally been an inability to identify which possibilities to prepare for and/or when or to what level to act upon them.

Table 1. Historical Examples of Surprise

Surprise Event	Cause	Result
Pearl Harbor	Not up to it, failure to imagine	Used depth and capacity
Kamikazes	Failure to imagine	Used depth and capacity
China enters Korea	Wouldn't dare, willing to take risk	Used depth, capacity, and nuclear deterrence
Sputnik	Years away, wrong value structure	NASA, DARPA, NRO
Bay of Pigs	Wouldn't dare, not up to it	Lived with Castro's Cuba
Cuban Missile Crisis	Didn't imagine, wouldn't dare	Stabilized under umbrella of nuclear deterrence
Tet Offensive	Not up to it, didn't imagine	Public support utilization caused withdrawal
Iran Hostages	Wouldn't dare	Failed rescue, loss of image
Beirut Barracks Bombing	Didn't imagine, misunderstood culture	Withdrawal, start long series of force protection measures
Victor 3/Akula Quieting	Undetected use of foreign technology	Prepared because we had anticipated capability in general
Soviet Bio-weapons Program	Misunderstood culture, did it to ourselves	Two decades of inattention
Kuwait Invasion	Wouldn't dare, wrong paradigm	Responded with Desert Shield/Desert Storm
Khobar, Cole, Nairobi	Didn't imagine, lost in other options	Pursue fugitives, stepped up attention to force protection
1993 World Trade Center	Too little imagination	Drew wrong lessons from "win"—9/11 discounted
9/11	Too little imagination, poor signal-to-noise	Modern tragedy, but not societal threatening—Operation Enduring Freedom, GWOT
PRC Force-down EP-3	Didn't understand risk calculus	Significant intelligence loss
IEDs in Operation Iraqi Freedom	Too little imagination, wrong paradigm	Tactical losses, strategic impact on public support
PRC ASAT	Not up to it, years away	Lots of U.S. activity, trying to understand motivations

As stated at the outset, U.S. military forces tend to deal very well with surprise at the tactical and operational levels. Because surprise is a fact of life in those environments, troops learn to accept the inevitability of surprise, to train for it, and to be highly adaptive to unplanned situations as they arise.

This facility to adapt does not, however, extend to surprise that occurs at the strategic or "existential" levels—that is, surprise that threatens the very foundation or existence of the country. At these higher levels, especially since the end of the Cold War and in the far more complex national security environment of today, we as a nation have been less well-prepared. What worked well as a deterrent strategy to prevent strategic surprise during the bi-lateral environment of the Cold War is not likely to be sufficient to meet the types of strategic surprise that could arise today, particularly surprises that may be brought about by rogue state or non-state actors who have acquired weapons of mass destruction. We therefore focused our attention in this study on the strategic or existential level of surprise.

Types of Surprises and Why They Occur

As briefly outlined at the beginning of the prior section, three domains characterize the manner in which adversaries most often create capability surprise:

1. Adaptation of new technology. Adversaries employ new, previously unused technology and adapt it to their needs. The United States is unaware of the new technology (which is not a common occurrence) or did not imagine (or more likely did not believe) that an adversary would employ the new technology against the nation.
2. Rapid fielding. Adversaries develop a new military capability using existing technology and transition it to a fielded capability much more quickly than anticipated. The United States may be aware of the development but is surprised by how quickly it emerges in the field—often assuming that adversary processes to field new systems mirror the lengthy ones in DOD.
3. Operational innovation. Adversaries develop a new and unanticipated operational capability by employing new tactics, techniques, and procedures rather than new materiel or weapons. Often this type of surprise emerges when existing equipment is used in ways that were not anticipated or for objectives that were not foreseen. In other words, the nation missed the signs, often contained in written doctrine or live exercises, indicating the potential or lacked the imagination to think "out of the box."

Surprise can also arise from a combination of the domains. In those cases, the primary surprise occurs at the intersection of two or more of them. Not only does the nation miss the signs within or between domains, but it also misses the fact that they were bound together with an integrative strategy that blended adversary strategic objectives, perception of U.S. strengths and weaknesses, and their own (not U.S.) cultural norms and preferences. Often, understanding these characteristics is a key to foreseeing a potential surprise before it happens. It is also a key to penetrating purposeful deception that often accompanies (and hides) an emerging surprise.

Why do these surprises occur, when in most cases there are events that foreshadow their occurrence? Generalizing from historical examples suggests the following reasons. The United States:

- Thought it could respond without doing anything new
- Knew it was likely, understood the magnitude of the implications, but didn’t pursue it appropriately
- Did not foresee the full consequences of an action and thus “did it to ourselves”
- Believed the adversary was not up to it
- Believed the adversary would not dare
- Knew it might happen, but was trapped in its own paradigms
- Didn’t imagine or anticipate the strategic impact
- Lost it in the “signal-to-noise” of other possibilities
- Imagined it, but thought it was years away
- Was willing to take the risk that it would not happen

As observed previously in this chapter, rarely is the reason that “we didn’t foresee it” or “we didn’t imagine it.” Instead, most of the events that have surprised our nation were foreseen in some way. The reasons for surprise range across the spectrum from misguided beliefs about the ability to respond, to erroneous perceptions about the adversary, to an inability to distinguish the probable from the possible, to a conscious willingness to accept risk attendant with inaction.

Lessons Our Nation Should Learn

Certainly the environment today differs from that associated with the many historical examples examined here. First, technology and globalization have empowered first- and second-tier states, non-states, and even individual extremists alike. Having the ability to "make really bad things happen" is no longer the sole province of a few major states. Moreover, moral or ethical norms by which the United States operates may be irrelevant to many potential adversaries. Second, growing social, cultural, religious, economic, and technical interdependencies have made it more difficult to predict national and regional unrest. There is greater instability in the world and the potential for unintended consequences is much higher. Finally, a key difference in the world today is reflected in the breadth of security challenges, the understanding of which demands deeper and more timely knowledge than the nation's intelligence, diplomatic, and investment capacities can provide.

Complicating matters even further in today's pluralistic world, a key step in preventing capability surprise is to understand an adversary's capabilities and intentions. The "penetrator" must be penetrated, using not only cyber means, but through a combination of the full instruments of national power—military, information, diplomatic, legal, social, intelligence, financial, and economic—to bring pressure, impose costs, or increase doubts on the part of an adversary. Given the fact that the nation states, groups, and even sets of individuals that represent potential U.S. adversaries are often not very well understood, assessing capabilities and intentions with any degree of certainty is a daunting task.

Despite the fact that today's world is significantly different from that of even a decade or two ago, leading to manifestations of surprise in new ways, the basic tenet of surprise has changed little, if at all. Surprise will happen! At the strategic level, if the United States does nothing to change its approach, the nation will remain ill prepared. It will also fail to anticipate strategic implications of seemingly lower level events.

To address what might be done to improve U.S. preparedness to deal with capability surprise, we have organized findings and recommendations of this study around the two categories of surprise alluded to above:

- *"Known" surprises*, discussed in Chapter 2, are those the United States should have known were coming, but for which it did not adequately prepare. For this category of surprise, the potential and evidence are clear; the effects are potentially catastrophic; and dealing with them is difficult, costly, and sometimes counter-cultural. They are, in effect, a "shame on us" if they occur.

- "*Surprising" surprises,* the topic of Chapter 3, are those the nation might have known about or at least anticipated, but which were buried among hundreds or thousands of other possibilities. In this case, the evidence and consequences are less clear, the possibilities are many, and the nation cannot afford to pursue them all.

In both cases, the biggest issue is not a failure to envision events that may be surprising; it is a failure to decide which ones to act upon, and to what degree. That failure results, at least partially, from the fact that there is no systematic mechanism in place within DOD or the interagency to help decide which events to act on aggressively, which to treat to a lesser degree, and which to ignore, at least for the time being. In other words, there is no mechanism for sorting, assessing, deciding, and responding. The lack of such a mechanism is central to the study's recommendations, summarized in Chapter 4 of this report.

Volume 2 of this report, Supporting Papers, contains self-contained discussions by each of the study's three principal panels—Technology, Transition and Fielding, and Operations—and provides considerably more detail on many aspects of the material presented in this volume.

Chapter 2. Known Surprises

"Known surprises" are distinguished by five characteristics:

- There is clear evidence that an adversary is developing a new hostile capability.
- That capability is relatively easy to acquire.
- That capability, when it materializes, has the potential to be very damaging to U.S. interests and/or military operations.
- The United States does not have a guaranteed way to identify or to punish the perpetrator, thus having no effective deterrent.
- The nation has not adequately prepared to prevent the surprise or to mitigate its effects.

Given all of these attributes, it should not be "surprising" that under the right set of circumstances, an adversary would employ this capability against our nation—thus, the somewhat oxymoronic characterization as a "known surprise." So why hasn't the nation adequately prepared to deal with known surprises? In most cases, it is because prevention or response is difficult, costly, and/or requires action that is counter to some institutional norm or culture. As a consequence, the United States remains vulnerable to an adversary capability that can cause severe harm, even though it may be possible to see it coming.

Fortunately, only a handful of surprise capabilities meet these criteria at the strategic or existential level. Three were identified in this study: cyber surprise, surprise in space, and nuclear surprise. All three have the potential to create serious damage to both the military and civil sectors. All three, particularly in recent years, are becoming easier to execute because the knowledge to do so is more pervasive and/or the technology or critical components are more readily available—either because materials can be adapted from civilian use and are therefore difficult to detect, or because weapons proliferation is not being effectively controlled. All three show indications of spreading as more potential adversaries are attaining capabilities. Conversely, none of the three, in numerous threatening scenarios, can be easily or definitively attributed, and, therefore, will be difficult to deter or hold off by the threat of retaliation.

All three are characterized, as well, by lack of adequate preparation on the part of the United States.

The members of this study debated the inclusion of a fourth threat—that of biological surprise. There is little doubt that biological threats fit the first four of the five criteria for a known surprise. What is less clear is how much more the nation should or could be doing to prepare for biological attack, since investments at the Departments of Defense, Homeland Security, and Health and Human Services have grown significantly over the past several years in comparison with the other threats cited. Further, the degree to which biological threats represent a military versus societal threat is also less clear. In the end, after much debate and discussion, we opted not to include biological threats in the analysis of known surprises.

Cyber Surprise

Over the past several years, DOD has become increasingly "net-centric." This entails networking many different sources of sensor and informational data with multiple processing nodes and geographically distributed users to achieve unprecedented levels of situational awareness, data distribution, and operational coordination. Net centricity requires changes in doctrine, organization, training, materiel, leadership, personnel, and facilities. A growing body of operational experience and exercise results point to the effectiveness of net-centric operations in a variety of situations.

The downside can be serious, however. Net-centric operations bring an increase in capability and increased dependence on the viability of the network, as well as the data contained within it. Thus, new vulnerabilities are created. Because information technology is ubiquitous in almost all war fighting capabilities, networks can reasonably be viewed by the adversary as the "center of gravity" for disrupting U.S. military capabilities. The knowledge and capabilities to attack networks are pervasive in much of the world—skilled individuals, equipment, access to networks—and the costs of such attacks are low. Further, not only is there a threat from the outside, but insider threats are a serious challenge as well. In essence, networks have become a combat capability and need to be defended as such.

Characteristics of cyberspace that create opportunities for exploitation include the following:

- Attacks can be launched remotely, with global effects.
- Attacks can affect not only information, but also physically damage equipment.

- Successful attacks can destroy user trust; once lost, trust is very difficult to reestablish, thus affecting all aspects of operational tactics and procedures.
- Attacks can be kinetic, but more likely non-kinetic, especially in "peacetime."
- Attacks are hard to trace or attribute, thus difficult to deter.
- Cyber-related infrastructure is becoming more and more homogenous.
- Attacks can be conducted autonomously, through "botnets" and similar activities; cyber attack vehicles can be communicable and self-replicating.
- Counters to cyber attacks often have negative consequences for the defender.

The velocity of change in cyberspace should make "operational surprise" not a surprise at all, but a condition that is expected and must be managed.

Preventing and Mitigating Cyber Surprise

In dealing with the potential for cyber attacks, the provenance of hardware and software needs to be addressed continuously throughout the product life cycle. Too often security activities focus on the operational phases, but today's global supply chain demands that security be addressed at each step, from concept development through end-of-life disposal. Security needs to focus not only on the hardware and software but on the cyber workforce as well. The assurance of operational networks and the data they contain depend on every operator being trustworthy. In addition, the network itself needs to be protected—knowledge about offense and defense capabilities, strong authentication and identification, and network mapping and discovery are all important toward that end.

Cyber capabilities also need to be more robust and enhancements need to proceed along several parallel paths. Capacity should be provided beyond expected needs. Diversity needs to be built into networks, support equipment, and operating systems to make success harder for the attacker. Networks must have the ability to be reconfigured rapidly and reconstituted under stress. Workarounds and fall-back procedures to achieve graceful degradation need to be defined, implemented, and practiced from the outset of network architecture definition. Critical subsystems and applications should have higher levels of assurance. And importantly, networks should be able to operate in degraded modes, with protected "high security" islands. In essence, functionality and excess capability need to be balanced with security.

Cyber mitigation is equally important. Attacks are hard to detect and to characterize, but these are essential tasks if cyber surprise is to be mitigated. Progress is needed in four broad areas:

- Collection and exploitation of operational data
- Distinguishing anomalous behavior or characteristics of systems, equipment, data, and people
- Having built-in techniques and procedures for rapidly recovering lost or anomalous data and reconfiguring networks for reestablishing integrity
- Strengthening tools for attribution

Other mitigation steps involve preparing for degradation across the dimensions of availability, integrity, confidentiality, authentications, identity, and trust. Plans and exercises should incorporate realistic degrees of degradation in each of these dimensions. Overall, the goal of mitigation measures should be to achieve mission assurance, not simply information assurance, so that commanders can continue to operate under all levels of attack. Lastly, cyber network attack against the adversary is another important element of the cyber tool kit and, to that purpose, attribution tools must be strengthened.

What is Being Done?

Steps to prevent and mitigate cyber surprise are being taken. But in the view of this study, these initiatives are in the early stages of implementation and are skeletal at best. Any significant operational improvements are yet to be achieved.

Perhaps the most significant of these is the Critical National Cybersecurity Initiative, which was launched by President Bush in May 2008. This initiative includes: (1) guidance on federal department assignments, resources, and government processes; (2) a strategy for near-term, mid-term, and leap-ahead initiatives; and (3) initiatives to develop cyber-related policies and to enhance deterrence. This major effort is comprehensive in scope, but not yet adequately funded.

The Department of Defense is promulgating new information assurance policies for the defense industrial base and actions have begun to increase participation of red teams, and to incorporate cyber and information operations in exercises and game play. While the inclusion of cyber considerations and attacks within red teams and war games is to be lauded, we remain concerned that cyber attacks never appear to go to the point of operational "breakage," and thus opportunities to assess the true degree of vulnerability, understand the corresponding impact on operational capabilities, and gain insight on how to mitigate or work around the loss or reduction in network and/or data integrity is lost. Within the classified domain, many developments are underway related to war-reserve approaches, hedging strategies and technologies, and ways to sustain trust, but the degree to which these have been matured and extended to all of the critical elements of DOD and related strategic civilian cyber networks is at best unclear.

An important area that is in its infancy is the need to share information and collaborate between the public and private sector. In some areas, such as the financial world and the protection of certain intellectual property, the private sector has seriously pursued the requirement for information assurance and engages in ongoing development of approaches that may be useful to DOD. It does not appear that these are being fully exploited by the Department. In terms of the private sector defense industry, the government has begun to provide industry with more information about threats to educate them, raise their level of awareness, and motivate preventive and defensive action.

The nation's cyber strategy is based on a mix of mature and immature approaches. More mature initiatives include perimeter defense, enclaves, black cores, key management, and public key infrastructure. Less mature elements of the strategy include initiatives in biometrics-based, non-repudiatable identity and identity management; the trusted computing initiative; and the ability to understand and control supply chain component heritage.

Cyber Progress after the Summer Study

Since the conclusion of the summer study activities in late summer 2008, the newly elected Obama administration, at both senior civilian and military levels, has shown a much heightened interest in dealing with the potential for cyber attack. In testimony before Congress, the Pentagon's top information security official cited a 6,000 percent increase over two years in attempts to penetrate DOD networks, from 6 million in 2006 to 360 million in 2008. During the winter and early spring of 2009 the following occurred:

- Upon the President's order, a 60-day review of the U.S. cyberspace posture was completed in May, resulting in a number of key areas for concern. These concerns have been echoed in statements by the President, who has announced the establishment of a new cyber security directorate within the National Security and Homeland Security Staff. In his announcement he said, "It is now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation." He said that we "were not as prepared as we should be" and that we had not invested sufficiently in protecting our digital infrastructure, which he described as a strategic asset.
- The Secretary of Defense announced in June 2009 the creation of a new multi-star multi-service cyber command as a subunit of U.S. Strategic Command. It will be led by the National Security Agency (NSA) director. Among other things, it will coordinate both defensive and offensive activities, something the Defense Science Board has been arguing for over the past several years. NSA likened the need for protection of cyber space to the nearly 200 year old Monroe Doctrine, which provides declaratory statements about those who would interfere with nations in the Western Hemisphere.
- Senate legislation in April 2009 pushed aggressively to dramatically escalate U.S. defense efforts against cyber attacks, including empowering the government to establish cyber security rules for private networks.
- The Pentagon announced plans to develop a simulated cyber world in which to try out and measure the potential effect of cyber weapons of mass destruction of tomorrow.
- The military service academies are conducting cyber war games as part of their curricula and training. These activities are expected to be extended more aggressively than is current practice to service and joint exercises and war games.

Although these efforts show greater attention being paid to the potential for cyber attack and what to do about it, it is still much too early to determine what the impact and efficacy of this increased attention will be. Hopefully, it will push beyond bold statements and bureaucratic actions, but, in any case, it is a promising sign.

Key Actions for the Future

While the steps described here are important and should continue to be funded and aggressively pursued, additional actions are needed to better position the Department of Defense given the inevitability of serious cyber attacks. As part of this study, members assessed the nation's current readiness against cyber surprise by evaluating capabilities to prevent, deal with, or create surprise. The assessment considered strategy, plans, and preparations. We concluded that both DOD and the nation are in a relatively weak state of readiness. In some cases, this is because current initiatives are too immature to have had an impact. In others, it is because there are still critical gaps in the nation's efforts. At a summary level, this study assessment concluded that the nation and DOD have only begun to deal with this threat seriously, present efforts by themselves are inadequate, much work needs to be done, and it will be very difficult and very costly.

The recommendations below focus on two areas critical to the Department of Defense that need a great deal more attention: the ability of the military to operate in degraded environments and increased protection of cyber capabilities.

RECOMMENDATIONS: CYBER SURPRISE

Chairman, Joint Chiefs of Staff, direct action on a series of exercise activities to gain operational understanding of the impact of cyber attacks:

- What and how deep are U.S. vulnerabilities?
- How do they impact the nation's ability to fight?
- How can the military fight through?

Vice Chairman, Joint Chiefs of Staff, direct the Services and combatant commands to initiate a series of activities to increase the resistance to cyber attack of critical information systems.

Iterate the two activities above to inform understanding of vulnerabilities, efficacy of corrective measures, and new measures that need to be taken.

Surprise in Space

As with cyber, the effective use of space is of critical importance to the United States. Yet vital assets exhibit increased vulnerabilities. The nation relies on space-based capabilities not only to meet the needs of joint military operations worldwide, but also to support diplomatic, informational, and economic efforts.

Space is essential to strategic and tactical military communications; missile warning; intelligence; and position, navigation, and timing. Commercial communications satellites provide direct support to U.S. war fighting forces. American citizens rely on space capabilities in many areas of everyday life—banking and financial, weather forecasting, GPS–assisted travel, recreation, and many others.

The United States, however, is not the only nation with heavy reliance on space. The number of nations directly engaged in space continues to increase, as does the capacity of many nations to contest space operations and capabilities. Techniques to deny the use of space are proliferating. Thus, space can no longer be considered the "safe haven" or sanctuary of the past. Instead, the United States should view space as a potential combat zone, where space assets can be attacked physically or electronically. In response, the national policy should drive development of both defensive and counter-space capabilities, consistent with U.S. treaty obligations.

Space situational awareness—the ability to see, assess, and understand activity in space—is increasingly important. It is also more difficult to achieve as satellites become smaller, debris becomes denser, and the nation's tracking systems continue to age.

Thus, as dependence on space has grown and challenges to the use of space have increased, the nation's ability to know what is happening has decreased. This combination of circumstances, coupled to an inability to deal with them robustly, establishes space as the second known surprise.

In reality, surprises in space have already occurred. The Chinese anti-satellite missile launch in 2007, which demonstrated an ability to challenge, disrupt, or destroy space assets and capabilities, is perhaps the best known due to the considerable press attention it received. But there are others as well. In 1962, satellite failures occurred in the aftermath of Project Starfish aimed at radiation effects enhancement of the Van Allen belt. In the 1990s, Libya successfully jammed communication satellites on a number of occasions. The nation should expect to face more significant surprises in the future. Unfortunately, like cyber, although the United States is taking some initial steps to address these challenges, the road ahead is long, difficult, and expensive.

What is Being Done?

Many prevention and mitigation activities related to U.S. space capabilities are ongoing today; some are described below. Among the most prominent are the following:

- A Space Situational Awareness Roadmap has been submitted to Congress.
- A Space Protection Strategy and Program has been developed.
- Initial efforts at addressing continuity of service for strategic communications; missile warning; and position, navigation, and timing are underway.
- The Operationally Responsive Space Office was established in May 2007.

Integration of effort. Integration and collaboration across the national security space community is essential and increasingly important, both within DOD and among other government agencies, industry, academia, and Congress. The Space Partnership Council, with diverse membership across the national security and civil space communities, is helping to share best practices, prevent duplication, and support integration of space activities. U.S. Strategic Command has established the Joint Functional Component Command for Space, providing a single commander with a global perspective that can enhance functional integration for the nation's space-based assets.

Launch surety. The United States recently completed its 58th consecutive, successful operational launch. A continuing commitment to mission assurance and exacting attention to detail is necessary to help enable assured access to space.

Missile warning. Space-based infrared sensing capability remains a critical requirement. In addition to the current Space-Based Infrared System (SBIRS)-High program, development of next-generation infrared surveillance systems should begin so that a range of options is available to ensure the nation's missile warning capability is both sustainable and responsive. Fielding capabilities on smaller satellites, for example, would increase the responsiveness of current capabilities, and is an option that should be explored. Here, as in other areas, an investment strategy and portfolio are needed that go beyond the current programs of record to support next-generation technical capabilities and emerging needs.

Communications. Continuity of service for strategic communications is essential even as the demand for high bandwidth capacity is increasing. The Advanced Extremely High Frequency communications program completed its first end-to-end communication test with legacy MILSTAR (Military Strategic and Tactical Relay satellite) terminals in June 2006, with first launch planned for 2010. The planned number of advanced extremely high frequency satellites has been increased to compensate for the recent cancellation of the Transformational Satellite Communications Program. The first satellite of the Wideband Global SATCOM (satellite communication) system is operational with plans to expand capability. Australia has entered into a partnership with the United States to receive high bandwidth capability from this system, and is providing key funding.

Position, navigation, and timing. The Global Positioning System (GPS) is the world's standard for space-based positioning, navigation, and timing (PNT). Assuring continued GPS capability is critical to the success of nearly all DOD missions and a wide assortment of civilian infrastructure capabilities. In 2006, interagency coordination of PNT matters was strengthened through an active National PNT Executive Committee, chaired by the deputy secretaries of defense and transportation, as well as through the establishment of the National PNT Coordinating Office. In addition, war fighter PNT capabilities are being improved through planned power and signal upgrades to GPS satellites, their ground control systems, and associated user equipment. Continued improvements in the GPS constellations, including new civil signals, more jam-resistant military code, new receivers, advanced processing techniques, and increased accuracy are ongoing needs.

Space situational awareness. Space situational awareness is the foundation for space protection strategies. Three systems are in development to expand or replace current capabilities: the Rapid Attack Identification Detection and Reporting System (RAIDRS), the Space Fence, and Space-Based Surveillance System. RAIDRS, being developed via a block approach, will provide initial capability to detect and geo-locate satellite communication interference. Follow-on blocks are planned to provide automated data access and analysis, data fusion, and decision support capabilities. The Space Fence will replace the aging Air Force Space Surveillance System. It will enhance terrestrial-based detection and tracking to provide capabilities for smaller radar cross-section satellites, increased satellite density and numbers, and broader spatial coverage, including the Southern Hemisphere. The Space-Based Surveillance System program is planned to deliver optical sensing satellites to search, detect, and track objects in earth orbit, particularly those in geosynchronous orbit. An acceleration of these programs and development of additional capabilities for the future are warranted in response to the rapidly evolving space environment.

Efficient acquisition. The "Back to Basics" initiative remains a key construct to improve space acquisition by promoting a renewed emphasis on increased discipline in the development and stabilization of requirements and resources, engineering practices, and management that includes a more deliberate acquisition planning strategy. It encourages a "block" acquisition approach where capability can be delivered through discrete, value-added increments as technological capabilities mature. Space acquisition approaches should continue to emphasize integration and collaboration among interested parties in all stages of the acquisition process to create partnerships within the space community.

Operationally Responsive Space Office. This office is focused on increasing the country's ability to launch, activate, and employ low-cost, militarily useful satellites to provide surge capability, reconstitute or augment existing constellations—or to provide timely availability of tailored or new capabilities. It is examining measures to achieve:

- Rapid small satellite design, development, and processing
- Rapid integration, launch, and on-orbit check out of replacement space assets
- Augmentation and reconstitution options including better use of existing fall back capabilities, including those in the ground and air
- The ability to transition rapidly from experiment to operational capability
- A high/low mix space architecture augmented with non-space assets

Further Action is Needed

Despite the ongoing activities described above, additional steps are essential. One is to implement a unified view of a robust national security space architecture. Within this architecture, U.S. Strategic Command should take the lead in stating formal requirements after vetting them within the Department, as well as with other government departments and agencies with relevant interests.

The nation also needs to develop options for a robust launch capability and accelerate planned improvements to space situational awareness capabilities. To be successful, sufficient resources must be provided for reliable operations in an increasingly important and contested 21st century space environment.

The Operationally Responsive Space Office needs to get beyond the organizational planning, assigning, and budgeting actions that have dominated its initial years and start producing real programs that will develop real augmented adaptation and reconstitution capabilities. In addition, it needs to develop and aggressively pursue a more expansive view of operationally responsive space, consisting of spacecraft, launch vehicles, and the ground segment to deliver a wider range of space options and effects to the war fighter. It does not appear that the charter for this office includes ground and/or air augmentation or reconstitution options. Further, it is also unclear where this responsibility does reside.

Even if the nation can create the integration and investment needed to redress current shortcomings in U.S. space programs, the international competition and threat environment is such that a "surprise" in space is highly likely. As such, the military services should be prepared to operate in space-degraded environments. Conducting games and exercises in such an environment is needed. In particular, U.S. Joint Forces Command needs to incorporate realistic, degraded space environments into all joint and combined war games and exercises so that war fighters gain experience operating under such conditions. In the longer run, reducing DOD's reliance on space capabilities and/or providing non-space workarounds and alternatives should be a priority.

RECOMMENDATIONS: SURPRISE IN SPACE

Chairman, Joint Chiefs of Staff, direct combatant commanders and military service chiefs to understand the operational impact of a degraded space environment and develop tactics, techniques, and procedures to fight through.

- U.S. Joint Forces Command should factor into joint/combined war games and appropriate exercises.
- U.S. Strategic Command develop foundational requirements to increase the robustness of the military space architecture across appropriate areas of awareness, assessment, protection, survivability, reconstitution, and fall backs.

Nuclear Surprise

The nation has not paid sufficient attention to the warning signs that, with respect to nuclear weapons, the "peace dividend" from the end of the Cold War is wearing increasingly thin. All declared nuclear powers, with the exception of the United States, are modernizing their nuclear forces in response to growing uncertainty in regional and international security environments. Contributing to these decisions have been attempts by some currently non-nuclear states to acquire a capability of their own—including states hostile to the United States and some of its allies. Interest on the part of non-state groups in acquiring nuclear weapons has added to these concerns. Even states that are choosing to remain at least overtly non-nuclear generally have the technology base to begin nuclear programs based on their ongoing investments in nuclear power. Should their vital interests become threatened in the future, these states could change their minds and begin nuclear weapons programs. Despite this potential, the United States has not been as persistent as it once was in reassuring other nations that its nuclear umbrella will be extended, should it prove necessary.

Of considerable concern among the many activities ongoing around the world are the rhetoric and actions of Russia and China. They both maintain a declaratory policy that they would be willing to use tactical nuclear weapons if necessary to stop an aggressor with superior conventional capabilities. The Russians have been open in their conduct of conventional force exercises from time to time in simulated tactical nuclear environments. The United States is no doubt at the center of the motivation.

Yet in the face of these external trends and actions, many prominent leaders in the United States still hold fast to the belief that no one would dare to use nuclear weapons against our nation—believing that no one would run the risk of U.S. nuclear retaliation. They hold to this belief despite the possibility that new generation weapons can create militarily useful human and electronic effects with less physical destruction, which can lower the barrier to use by others, especially on their own territory. They hold to this belief despite the potential for being drawn into regional conflicts after limited use of nuclear weapons against U.S. allies. And they hold to this belief even as others see the United States as "self-deterred" based on public statements by key civilian and military leaders alike to the effect that they cannot imagine U.S. use of nuclear weapons. The rhetoric is accompanied with a lack of investment in force modernization.

Is the United States setting itself up for a serious "surprise"?

Current U.S. Situation

Over the decades of the Cold War, the United States worked to understand the many avenues for deterrence. It backed up policies and diplomacy with offensive forces and defensive capabilities that enabled our nation to hold at risk the valued assets of adversaries. The United States has yet to replace the Cold War strategy with one more relevant to the current era, but the basic elements of "carrot and stick" still pertain. In that context, there are worrisome warning signs that the capabilities that provide the foundation of U.S. deterrent policies—applicable to both the United States and its allies—may be eroding.

Twenty years of underinvestment in the health of the nuclear enterprise at both the Departments of Energy and Defense are, not surprisingly, taking their toll. Both the people and the weapons systems are aging. Delivery platforms are approaching the end of their useful service life. An increasing number of individuals with expertise gained through decades of experience have retired or are nearing retirement age. Yet no plans have been developed to refresh these capabilities. A critical part of the problem is that the nation's leadership, especially in the military, has continued to downplay and under support the nuclear mission. Serious, recent operational missteps are evidence of a lack of importance placed on the nuclear mission.

On the defensive side, the nation continues to hold to the belief that American men and women in uniform will never fight in a nuclear environment. As a result, nuclear survivability of critical conventional war fighting capabilities is a very low priority. In turn, this view has led to a near total collapse of the nuclear effects part of the enterprise. Military attitudes are inimical to dealing with "fighting through" the use of nuclear weapons on the battlefield. War fighters lack knowledge in how to operate in a nuclear environment because they do not receive even the most basic education and training. Lacking any "demand pull" from the military, the technical expertise and facilities that have provided support in the past have all but disappeared. The expert technical workforce in radiation effects, once robust, is virtually non-existent today.

In the realm of treaties and agreements to stem proliferation and control nuclear materials, the nation has seen an episodic approach by the past two administrations. The renewed emphasis that the new administration is placing on arms control and nonproliferation is a needed and welcome change, but lessons from the past indicate that hastily struck agreements should be avoided. The low level of diplomatic efforts for the past 15 years has been accompanied by little investment in advancing U.S. monitoring and verification capabilities, as well. Today's challenges are far more complex than they were during the Cold War—a time when the numbers of weapons and delivery platforms were greater, and the United States could direct its focus primarily on the Soviet Union. Detecting and monitoring low numbers held by more players presents a significant technical, not just diplomatic, challenge in the current environment.

This environment of neglect also stems from a less than compelling attitude on the part of the nation's senior leadership in both the Congress and Executive, in which an impasse on how to move forward has existed for more than a decade. While senior leadership in Congress and two prior administrations have voiced their belief that nuclear weapons must retain an important and enduring role in the nation's security, they have failed to prioritize and fund activities that would modernize U.S. capabilities and maintain the viability of that enduring role. The two prior Nuclear Posture Reviews have failed to provide a foundation for a nuclear strategy and, hence, little meaningful action has followed.

The life of existing weapon systems, both delivery platforms and the warheads themselves, has been extended for the past two decades. But life extensions cannot continue indefinitely. Modernized capabilities are needed, but replacements will take, in many cases, longer to produce than the remaining life estimated for current deployed capabilities. Despite these facts, and a joint commitment among the Departments of Defense, State, and Energy of the last administration to modernize the force, the Reliable Replacement Warhead—critical to nuclear competence—has not been approved by Congress. Furthermore, even the exploration of concepts for new or modernized capabilities has been prohibited. Not only have offensive capabilities been under extreme scrutiny and criticism, but defensive programs focused on nuclear protection have been as well, including the Department of Homeland Security's programs in nuclear defense. It remains unclear whether the latest Congressional Strategic Posture Commission[1] will catalyze consensus, followed by action.

Today's multi-polar world has complicated the deterrent rationale for nuclear weapons, as well as introduced potential conflict situations in which their limited use might be threatened by others. There remains the need for a nuclear arsenal as a hedge against the uncertainties that the complexities of the international environment present. But U.S. actions do not appear in many respects to support this need.

What is being done to improve this situation?

Although inadequate, a few positive steps have been taken. Notable examples include the following:

- The Stockpile Stewardship Program, initiated in the mid-1990s by the predecessor offices of the Department of Energy's National Nuclear Security Administration (NNSA), has produced an impressive set of above-ground simulators and high-end computational hardware and

[1] "America's Strategic Posture," *The Final Report of the Congressional Commission on the Strategic Posture of the United States*, William J. Perry, Chair, April 2009 (United States Institute of Peace Press). The Commission calls for a balanced approach to nuclear issues, one that re-energizes nonproliferation and arms control efforts, along with credible offensive and defensive capabilities, akin to what the Defense Science Board recommends here and in other reports. It recommends that both the strategic triad and the Department of Energy's nuclear weapons complex be maintained for the foreseeable future, but doing so will require significant investment.

software that is enabling some degree of continued validation of existing weapons, without underground testing.

- The Secretary of Defense sent a strong message about the importance of the nuclear mission when he replaced both the Air Force Chief of Staff and the Secretary of the Air Force in the wake of missteps by the Air Force in 2007 and 2008 in executing their nuclear responsibilities.
- An expanded memorandum of understanding between the Defense Threat Reduction Agency and NNSA is seeking to revitalize the nuclear weapons effects technical community.

But for the most part, the nation continues to simply study the problem, as it has been doing for more than a decade. These efforts are not only insufficient, but also unlikely to affect sustained change throughout the nuclear enterprise unless the nation's leadership, at the highest levels, continues to place value on and emphasize the importance of the nuclear mission.

A Greater Commitment is Needed

This study offers an abbreviated set of recommendations that build on the work of many Defense Science Board studies and other efforts that have addressed this topic.[2] At the top of that list is the commitment of the new administration's leadership to place nuclear weapons as a priority in national security policy and strategy. It is not necessary to return to the dominant role of nuclear weapons during the Cold War. Instead, these weapons should be viewed as the nation's ultimate "insurance" in a world of uncertain, risk-laden environments.

As a result of the inherent uncertainty in today's security environment, many things can and should change—force structure, force sizing, and an increase in international treaties and cooperative measures, to name a few. The tendency now, as in the past, is to focus on the numbers, but that misses the important inter-relationships among all the factors that impact the ultimate goal of deterrence. The next Nuclear Posture Review should address these and the many other issues related to nuclear capabilities that have been neglected in terms of their relevance to today's security challenges.

[2] The *Report of the Defense Science Board on Defense Imperatives for the New Administration*, August 2008, contains a summary of key Defense Science Board findings and recommendations in this area as well as a list of more than 35 articles and reports published over the past decade.

RECOMMENDATIONS: NUCLEAR SURPRISE

The administration reestablish a focus on nuclear issues as a top priority in national security policy and strategy. It must:

- Develop a comprehensive strategy analogous to what evolved during the Cold War, but relevant to 21st century multi-lateral issues
- Actively engage Congress to develop a bipartisan consensus

The Secretary of Defense direct that implementation of the next Nuclear Posture Review be given priority by senior military and civilian leadership:

- Establish needs, programming strategies, and resources for modernizing critical force elements (Office of the Secretary of Defense, Air Force, Navy)
- Direct that critical war fighting and support functions be assessed for nuclear survivability, and that measures be taken to ensure mission success in the wake of a nuclear attack (Under Secretary of Defense for Acquisition, Technology and Logistics; Vice Chairman, Joint Chiefs of Staff)
- Reestablish valued career tracks for nuclear expertise (military services)
- Re-introduce nuclear issues into education, training, gaming, and exercises (combatant commanders, military services)

Addressing Known Surprises: Overarching Recommendations

A reasonable person might wonder why the United States has been so reticent to vigorously address these three threat domains. There are clear signs that serious challenges, if not attacks, based on some of these threats are already upon the nation and, that whether upon us now or not, each of them has the future potential for great harm and disruption. The reasons are many:

- “Fixing” these known surprises is very difficult: they are tough problems, it is not clear how much is enough, and improving the situation is very expensive.
- The United States has not been hurt badly enough yet.
- Sometimes it is difficult to distinguish the “merely important” from the “crucial.”
- Objective measures of success are, at best, elusive.

- There is an unwillingness to expose weakness to learn how to fight through.
- Understanding of the problems is not pervasive within the political leadership.
- It is difficult to distinguish valid commercial activities from military applications.

Beyond these reasons of cost and complexity, poor understanding, and unwillingness to expose weaknesses and vulnerabilities, each of these threat modalities has special concerns, such as the enormous policy issues associated with moving forward on improving the nation's nuclear capabilities; a different but equally significant set of policy issues associated with dependence and vulnerabilities in space; and the proximity and interaction of civilian and military use of cyber systems, defense, offense, and warfare. Further, these capabilities and the issues that impact them are not mutually exclusive. Thus, there are additional complexities that arise in trying to deal with the challenges in one area without addressing challenges in the others.

Ultimately, the single most important requirement for making progress on each of the three known surprises addressed in this chapter, and others that may arise in the future, is the leadership provided within the Department—leadership that makes it clear that these are very serious threats to the nation that cannot be brushed aside and must therefore be dealt with aggressively.

Progress must begin with action on the part of the Secretary of Defense. The Secretary must be totally unambiguous in stating that before the nation ever gets surprised by any of these modalities, it is critical to fully understand the risks and opportunities in this small set of areas; establish appropriate actions, plans, and schedules for mitigating the former and exploiting the latter; and putting in place measures that can be used to quantitatively assess progress. In addition, it is essential for DOD's civilian and military leadership to bring Congress on board as a partner in understanding these issues and what is needed to deal with them—in terms of policies, programs, and investments in both people and funding.

In essence, these overarching recommendations for addressing known surprises can be summed up in a single word: leadership. Leadership is essential to understand the threat, to assess the options, and, most important, to take appropriate actions to prevent attacks and mitigate the impact should an attack occur.

OVERARCHING RECOMMENDATIONS: KNOWN SURPRISES

The Secretary of Defense establish a formal mechanism to ensure Department progress in addressing the limited number of most critical threats—the known surprises. The Secretary direct:

- An ongoing assessment of the risks posed by these known surprises: foreign capabilities, U.S. strengths and vulnerabilities, and net potential consequences
- A series of operational exercises, games, and red teaming activities that both inform and reflect the risk assessment
- Identification of a series of measurable goals/time frames for improving our abilities to deter; fight through; detect, prevent, and mitigate; use appropriate offensive measures

The Secretary of Defense and Chairman, Joint Chiefs of Staff, engage and educate congressional leadership on these issues.

Chapter 3. Surprising Surprises

We now turn our attention to "surprising surprises," those for which the evidence and consequences are less clear, the possibilities are many and buried among hundreds or thousands of other possibilities, and the nation cannot afford to pursue them all.

As pointed out at the beginning of this report, rarely is there a case of true surprise, at least in the classic sense. Post mortems almost always indentify that someone had provided warning, but that the warning was not heeded. The reasons can be many, but most often, before a particular surprise presents itself, it is typically obscured by many other, equally plausible—or implausible—possibilities, none of which stand out from the rest. Given that the nation cannot afford to address every possible "surprise," this study aimed to define an approach that would enable the government to systematically decide which potential surprise(s) should be addressed and how.

Part of the answer to this question can be found in the military's general approach to planning, equipping, and training. The military develops and practices war plans aimed at prevailing in a range of situations for which operational and strategic outcomes favorable to the nation's security goals are met. In parallel, the nation's military superiority is expected to prevent many wars from occurring in the first place.

Experience has shown, however, that conflict rarely progresses as planned. As a result, both military leaders and forces in the field are trained to adapt and deal with the situation at hand. The nation's strategy is aimed at prevention for those threats that are the most threatening, while agility to adapt and address the unexpected "in the moment" is emphasized in tactical and operational training.

This traditional perspective toward surprise is problematic, as has been observed through experiences in Operations Enduring Freedom and Iraqi Freedom, because distinctions among tactical, operational, strategic, and even existential levels of war fighting are blurring on today's battlefields. Tactical events can quickly turn into strategic issues—the use of improvised explosive devices being one poignant example. Thus, in not having anticipated such possibilities and their potential impact, the nation finds itself surprised, and too often at a cost of lives lost and goals unmet.

Managing Surprise

During the course of this effort, the study team explored organizations that seemingly manage surprise well. Included in that set were various science and technology groups charged with avoiding technological surprise, private sector firms recognized for innovative product development and sustained financial performance in competitive markets, successful hedge fund managers, and another nation's approach to national security planning (the United Kingdom). A comparison of the practices of these various organizations to those in the Department of Defense showed that the Department does in fact have some of the elements that might contribute to effective surprise management. Yet, many key ingredients are also lacking. In addition, even if all of the individual elements existed, there is currently no effective means for integrating among them. In other words, the Department lacks a process for managing surprise.

The study identified five steps that, integrated together, constitute a robust approach to managing surprise:

- A scanning and sifting process that narrows the many possibilities to the most worrisome few
- A "red" capability projection function that takes a "deeper dive" on the worrisome few through analysis, simulation, experimentation, and/or prototyping
- A net assessment process in which the deeper understanding of "red," gained through capability projection, is played against "blue" capabilities in order to assess the degree to which the nation can address the threat or adapt capabilities already in hand
- An options analysis team to provide an unbiased evaluation—or "rack and stack"—of the alternatives should blue capabilities prove inadequate
- An ability to produce a decision package that can be acted upon by senior leadership

As illustrated in Figure 1, an integration function links the steps together and then iterates continuously in order to account for new knowledge and the dynamic set of adversaries that the nation faces. Surprise can be managed—not to prevent it from occurring, because that is not a realizable objective—but rather to hedge against higher risk possibilities and, equally important, to create the agile mechanisms that should allow more timely response should the unexpected occur.

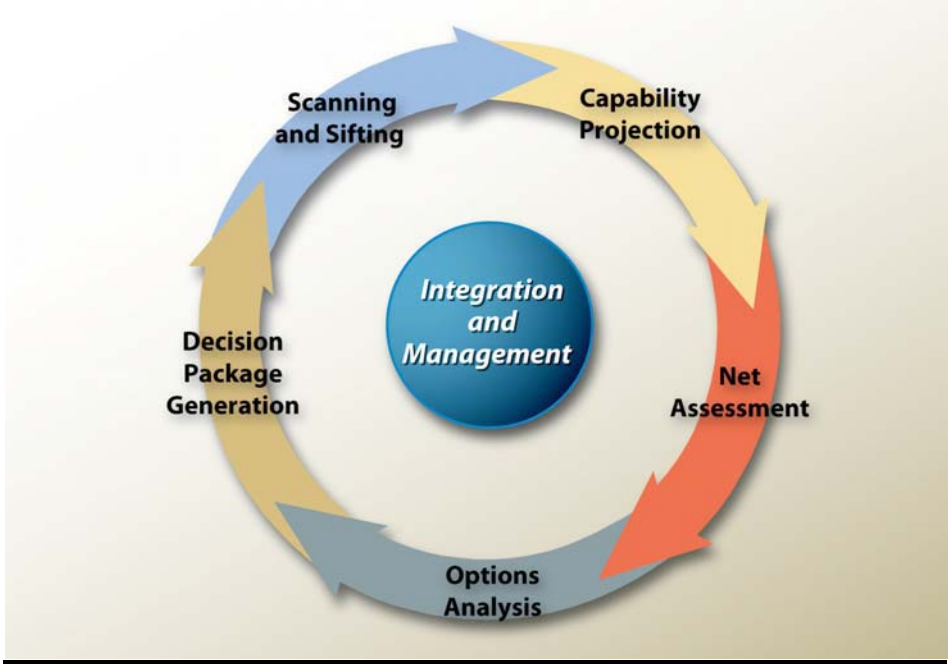


Figure 1. The Surprise Management Cycle

Scanning and Sifting, and Capability Projection

Technology development today takes place in a global environment of collaboration, funding, intellectual property protection, security, recruiting, mergers and acquisitions, and across boundaries created by governments and business and academic communities. As a result, conventional approaches of geospatially-based intelligence collection and detection need to be supplemented with new techniques that are both more comprehensive and more integrative.

Historically, the space of technical innovation has often been described by domain taxonomies: nested lists of technical domains and sub-domains. While useful in support of planning and budgeting, these taxonomies can be less useful in actually managing surprise, for which flexible design processes are needed to address many domains—including the goal to anticipate new developments as they emerge. A potentially more useful approach to anticipating technical advances—that is, for scanning and sifting in the context of the technical aspects of capability surprise—is to focus on the most innovative people and the relationships among them, both institutional and social. These networks provide the infrastructure through which ideas and experience flow and are facilitated by access to funds and end-users. Identifying and understanding the activities and interactions of the leading researchers will provide insights that should facilitate anticipating breakthrough developments that result in surprise.

This approach to following technical innovation is far more difficult today, however. Both the numbers of people engaged internationally and their individual and collective output is broader, more distributed, and more extensive. Instead of focusing on scientific developments by a single adversary, the country must now consider a highly diverse set of related but uncoordinated technical activities worldwide. Instead of a small, select international technical population, the nation must now deal with researchers all over the world.

The current U.S. intelligence collection and analysis tools simply do not scale to this new reality—the ability to connect technology advances with potentially threatening capability is lacking. Creativity is called for in at least three dimensions:

- Exploitation of new classes of signatures, especially from open sources
- Imaginative use of emerging technologies to vastly increase the productivity of intelligence analysts, allowing them to cover the larger target set and to absorb the vast amounts of potential new signature data available
- Continuous adjustment of the areas of most intense observation, both within the analysis process and through direction of collection efforts

All three dimensions fit into a “coarse-to-fine” paradigm, monitoring all known activities at a coarse “horizon scanning” level (see sidebar text box), and then selecting for greater “technology watch” attention those efforts that are deemed likely to create a significant threat. “Technology watch” domains will frequently emerge and change, so their selection should not be permanently established in any formal organizational construct. A parallel effort in understanding organization and intent, to the extent that such monitoring is possible, should accompany the technology track of the scanning and sifting process. The range of actions from a scanning and sifting process includes:[3]

- *Do nothing*, as there is no apparent threat. The topic is not discarded, but rather placed on a back burner to revisit in later cycles.
- *Follow commercial advances and applications*, as progress will likely outpace any government effort. Continue to ask if the products could be used in harmful ways that might not be expected.
- *Further assess* to better understand and/or quantify intriguing, but highly speculative, "weak signal" areas. Further research should be conducted to fill in gaps in knowledge.
- *Take a "deeper dive,"* if the risk appears high enough, to quantify, evaluate, and/or demonstrate key aspects that would be threatening—that is, move beyond scanning and sifting to capability projection.

In all cases, better intelligence is likely to be needed. A benefit of the systematic nature of the scanning and sifting process is identification of key indicators, which in turn can be the basis for more focused tasking to the intelligence community.

Capability projection, as the study conceptualized it, would have many of the elements of creativity and innovation typical of DARPA's efforts, but with a distinctly "red" emphasis that seriously tests "blue" concepts and capabilities. Capability projection would use all the tools of operations and systems analysis, system engineering, and design to map technology advances in the "deeper dive" category into a military operational context. This process would need to be supported by a strong interaction with red teams throughout the Department. The red teams would be challenged to postulate new capabilities from the spectrum of technology alternatives. Any effort in capability projection must also be influenced by input from the combatant commanders and military services to be inclusive of new capability projections from many sources. Finally, unanticipated "pop-up" threats would be subject to an initial assessment and, if serious enough, would be added to the set of potential capabilities for more complete capability assessment.

[3] The study adapted these outcomes from a process employed in the United Kingdom by the Defense Science and Technology Laboratory.

Horizon Scanning

The horizon scanning function, as the name implies, looks across the capability horizon in a "breadth first" fashion. Its information sources include open technology and military research literature, critical capability assessments, and both national and DOD strategy and technology plans. A key input to horizon scanning is data on emerging capabilities that are identified by the intelligence community. A core team (with outreach support) sifts through this information to provide alerts, spot trends, and populate research networks. The horizon scanning process produces a mixture of technologies and capabilities. Horizon scanning requires data on a broad range of technical activities—to include geographical, scientific, and observational elements. To achieve effectiveness across this range, horizon scanning is targeted on the two signatures common to all of the above: people and institutions generating innovative technical ideas. This breadth provides pointers to identify innovative new concepts, emerging fields of endeavor, diverse funding arrangements, and dissemination mechanisms that connect the network.

The challenge of using horizon scanning tools at scale is finding weak signals in the enormous volume of open source and cyber data. In 2003, the Organization for Economic Cooperation and Development (OECD) estimated that over 600,000 articles appeared in the scientific literature. Manual exploitation of this volume of source data would be prohibitive. A comprehensive suite of automated exploitation tools, largely developed under the sponsorship of the Defense Advanced Research Projects Agency (DARPA), has matured over the last decade to provide a basis for this approach.

In 2002, a seminal paper by Barabasi titled "Evolution of the Social Network of Scientific Collaborations"[4] opened the field of scientometric analysis. Subsequent work has strengthened and adapted social network analysis models to identify emergent behavior of very weak networks. These tools are routinely used today in the field of bibliometric analysis to identify the size and relative impact of research groups. This approach, which is one that the study reviewed and recommends for consideration, has resulted in horizon scanning and technology watch tools that are in use at the National Ground Intelligence Center and the United Kingdom's Defense Science and Technology Laboratory (DSTL).

Features of these many exploitation tools include the ability to continuously catalog web content, translate foreign languages to English, extract entities and relationships from text data, convert speech to text, and generate alerts when specified linguistic patterns appear. The results are in the form of machine-readable output that can support additional automation in downstream processes. Coverage gaps in traditional media can be closed by exploiting global connectivity to access additional cyber data. Data from these new sources can be processed in an automated fashion, without corresponding increases in staffing. Early research has captured salient content from the network and is beginning to explore the possibility of identifying emergent intent.

[4] A. L. Barabasi, H. Jeong, Z. Neda, E. Ravasz, A. Schubert, and T. Vicsek, "Evolution of the Social Network of Scientific Collaborations," *Physica A: Statistical Mechanics and its Applications*, Vol. 311, No. 3–4. (15 August 2002), pp. 590–614.

Unfortunately capability projection activities are limited throughout the Department and present a significant gap for effective surprise management. The most notable successful example of ongoing capability projection is the Air Force Red Team, which has existed for several decades. The Navy's "Deep Red" effort was established several years ago following recommendations of a previous Defense Science Board study. This analysis effort, which is part of the OPNAV intelligence staff, has produced some noteworthy (albeit classified) results, but its influence appears to be highly dependent on naval senior leadership and/or combatant commander interest. The Army Materiel Command has proposed a "Red Design Bureau," an effort similar to the Air Force Red Team, based on recommendations from the Army Science Board. But, at the time of this study, no funding commitment had been made to support the effort.

Net Assessment, Options Analysis, and Decision Packages

After the scanning and sifting activities have identified the most worrisome potential capability advances, and capability projection efforts, aided by red teams, have postulated the use of technologies to create potentially challenging new capabilities, there is still additional work to be done to prepare options for action by the senior decision-makers within DOD (Figure 2). Specifically, the capability projections should lead to a formal net assessment that draws on an understanding of strengths and weaknesses of both the United States *and* its adversaries.

The first step in the net assessment process is to generate candidate U.S. strategies to counter postulated adversary capabilities through systems analysis, operations analysis, and simulation. The same techniques are used to assess the net impact of candidate strategies and, if improvements are possible, to refine them. In some cases, there will be a need to augment simulation and analysis with experimentation. The technical experimentation performed as part of capability projection will answer the question, "Can this really be done?" Within net assessment, operational experimentation, if employed, will answer the question "Can they really use this and, if so, will it make a difference?"

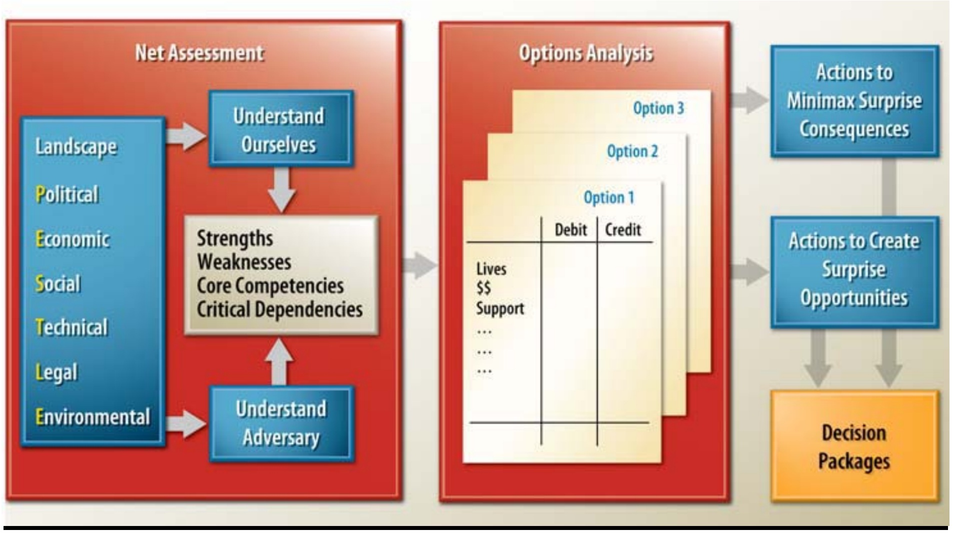


Figure 2. Net Assessment and Options Analysis Elements in Managing Surprise

An output of the net assessment will be the classification of emerging capability surprise areas into categories, such as those:

- That can be handled by existing or readily adapted U.S. capabilities
- For which there is insufficient evidence to require addressing immediately, but which should be watched for further developments, and should be tasked as potential targets to the intelligence community
- That create serious future risks for which capability gaps exist and need to be addressed

For this latter category in which capability gaps exist, the net assessment should inform a process that develops multiple options for addressing each potential capability surprise—either by taking actions to mitigate the impact of the adversary developing and employing the new capability, or by taking the initiative and exploiting the capability offensively to produce a surprise for the adversary. Creating this range of potential options may require detailed technical experimentation, acquisition planning, and review of training and doctrine alternatives.

After being defined, the alternative actions need to be evaluated via a top-level, systems-based, cost-benefit analysis, with the results being presented in a decision package for senior leadership in the Department.

These decision packages should not only present the rationale for the recommended course of action, but also provide a good summary of all alternatives considered so that senior leadership can understand the full context and rationale for the recommendation, as well as being able to explore alternatives and consider additional factors that the options assessment team may not have been aware of.

Enabling Activities

The surprise management cycle does not operate in isolation from other activities in the Department. In addition to the core elements illustrated and described in the previous sections, there are many other ongoing activities with which the cycle should interact. For example:

- DOD strategies and critical capabilities provide input into scanning and sifting activities.
- The intelligence community provides input into scanning and sifting activities on adversary capabilities and intent.
- Capability projection is informed by the research and development (R&D) community, but various activities ongoing in the combatant commands and military services, as well as incidents that may pop-up during the course of assessments, could influence this process.
- Net assessment is informed by gaming, exercises, experimentation, and formal assessments that are ongoing throughout the Department, such as in the Office of Net Assessment and through the Joint Experimentation Program at Joint Forces Command.
- Red teaming interactions can influence any of these elements and serve as valuable input to the various analyses.

Shortcomings in Managing Surprise

Adding in the enabling activities and decision options to the surprise management cycle produces a complex process (Figure 3). To be effective, it must be managed. When looking at capabilities within the Department to manage such a process, the task force found many shortcomings; in particular:

- Some elements of the surprise process exist, but are not oriented towards addressing capability surprise.

- Some elements of the surprise management process cannot be found anywhere in DOD today.
- Whether individual elements exist or not, there is no organization with responsibility for integrating among them or managing the entire process.

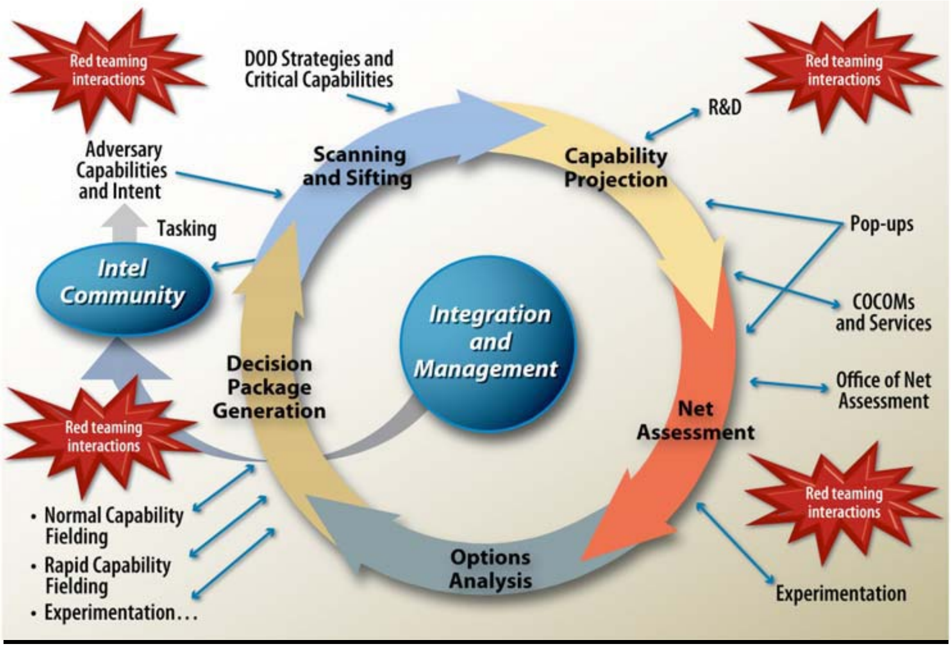


Figure 3. A Complex Integration and Management Challenge

For example, the Office of Net Assessment is a long-standing organization highly respected for its work, which is analytical in nature. But its scope is not as broad, nor its role as formal, as this study believes is needed for high-level decision-making in managing surprise. In addition, robust red teaming that would challenge a wide spectrum of blue capabilities, for the purpose of learning and improving them, is simply not practiced anywhere in the Department beyond the tactical level.

With respect to options analysis in the context of preventing, mitigating, or dealing with surprise, no current organization has the responsibility for unbiased, traceable analyses of options across the spectrum of doctrine, organization, training, materiel, leadership and education, personnel, and facilities. The more common practice is to allow the champion of a given concept to undertake his or her own analysis of alternatives. The inevitable result, not surprisingly, is that the alternatives are “gamed” to produce the going-in, desired result.

Even with a careful, dispassionate options analysis that could motivate a good decision, the Department lacks a number of tools and approaches that would enable a range of possible actions once a decision is made. For example, there are many rapid acquisition organizations but they are highly variable in their practices and focus.[5] Instead of enforcing a sunset for these organizations when their original purpose has passed, the Department tends to establish a new one for the next job at hand—leading to typical start-up pitfalls and relearning, while adding to the proliferation of special purpose, often sub-optimal, organizations.

It may also be that the best decision is to learn more through experimentation and red teaming, yet red teaming is not common. Irrespective of what form the decision takes, desired actions will almost always include a need for better intelligence, but few are skilled at providing focused requests to which the community can respond and/or develop the means to respond.

Even if all these elements existed, one has to go all the way to the Secretary of Defense to find the alignment of accountability and responsibility for bringing them together.

The following chapter describes the steps needed to redress the principal shortcomings identified here and improve the Department’s ability to manage capability surprise.

[5] Not only are they “many,” but due to semantics and sometimes fuzzy descriptions, they are often difficult to identify and/or differentiate. Recent studies place the number, depending upon how one counts and defines, anywhere between the low 20s and the high 30s.

Chapter 4. Redressing the Shortcomings

In the assessment of the study team, the Department must take several important steps to effectively manage capability surprise:

- Integration and management of surprise at a high enough level to affect senior decision-making
- Red teaming as the norm instead of the exception
- Rapid fielding that is truly rapid and can be effectively employed
- Pointed improvements in "strategic" intelligence

Addressing each of these areas individually is difficult enough, much less as a set. But planning under uncertainty has become the norm, which in turn calls for new and/or different approaches and institutional processes. Without a shift, the nation can expect to continue to be surprised—and likely with greater frequency and higher consequences.

Integration and Management

As illustrated in Figure 3 (Chapter 3), a strong integration and management function is required to link elements of the surprise management process together. The nature of surprise is complex—or "wicked" in the terminology of a growing body of research focused on seemingly intractable problems. Wicked problems are characterized as complex, multivariable, highly non-linear, and having no set solution.[6] These problems involve many stakeholders with competing viewpoints and goals. They are not easily solved, as implemented solutions have impacts on other aspects of the problem, thereby creating an environment where the search for solutions never stops. The kinds of wicked problems dealt with here need to be managed through a process characterized by the following:

- Expanding the problem to its full dimensions—that is, formulating the entire "mess" before seeking solutions (scanning and sifting)
- Understanding adversary motivations, intentions, and capabilities (capability projection and red teaming)

[6] Appendix A contains an overview of the concept of, and approach to dealing with, wicked problems.

- Being open to outcomes and anticipating the unacceptable (options analysis)
- Remembering past failures, since success will be fleeting because the adversary has learned and adapted (net assessment and iterating the process)

To formally introduce this management process into the Department of Defense, the study recommends creating a high-level, centralized organization with responsibility for addressing, and to whatever degree possible, preventing surprise. Toward that end, the Secretary of Defense should charter a Capability Assessment, Warning, and Response Office (CAWRO). The mission of this office is to provide the Department's senior leadership with timely assessment and warning of significant potential red capabilities, their impact on future U.S. operations, and courses of action to counter them.

The CAWRO should have the following features (Figure 4):

- A very wide input space. The CAWRO needs to proactively scan the potential capability landscape to find and postulate new adversary capabilities.
- A decision package output product. The CAWRO must produce response options that are both effective and affordable within operational and budget constraints.
- An assessment capability with both active feedback and continuous updating with new inputs. The "capability sets" of the nation's adversaries are not static. Similarly, U.S. capabilities are changing. The CAWRO needs to be constantly aware of the dynamic capability landscape when assessing potential adversary capability impacts.
- A high-trust two-way relationship with senior DOD leadership. The CAWRO will produce warning of mismatches and/or shortfalls in investments, people, and/or operational preparation. It will be easy for this information to be perceived as "bad news" or evidence of nonperformance by other organizations within the Department. The "news" needs to be prudent, credible, and trusted, but should also come with options for remediation.
- A protected budget. The CAWRO's continued existence cannot be threatened by the impacts of its products. It is important that the Department have a continuous source of "constructive bad news" as a key

part of a surprise-hedging strategy. Much of the Department will see it as their duty to marginalize the CAWRO—it must be protected from that.

- Significant connections to the intelligence community. To accomplish CAWRO's broad reach, an active (and intimate) relationship with the intelligence community is required. The horizon scanning performed by CAWRO needs to consider what adversaries know about the United States and the level of confidence in that knowledge. In addition, in a constantly shifting capability landscape, the set of indicators of new capabilities are dynamic. CAWRO must be informed by—and likewise inform—the intelligence community's capability collection and analysis process.
- Connectivity to red teaming. CAWRO needs to have strong connectivity to the red teaming activities ongoing throughout the Department to ensure that adversary capabilities, creativity, cunning, and sometimes very different culture and objectives are well represented. The CAWRO is the advocate of complex adaptive threats, as opposed to just the validated ones. (Additional recommendations on red teaming will be addressed later in this chapter.)

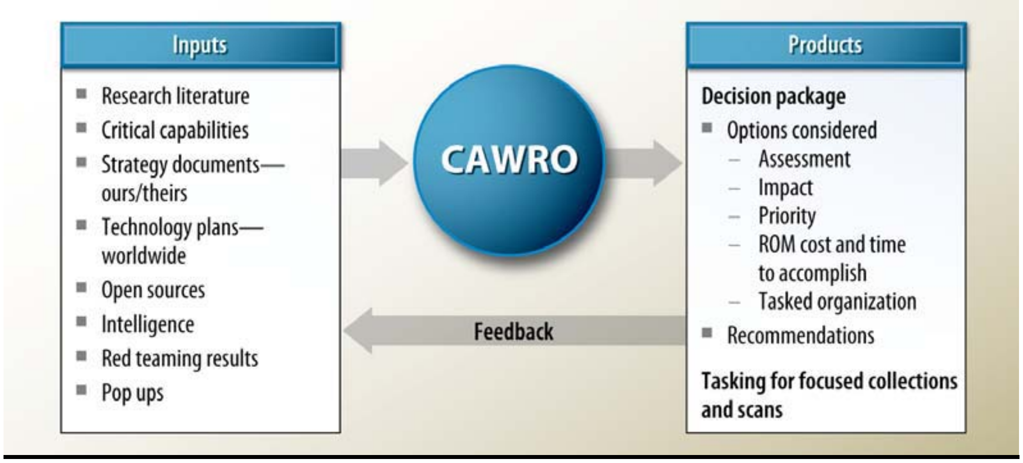


Figure 4. Inputs and Products of the CAWRO

Structure

There are two major parts to the CAWRO: threat capability assessment and response generation. Accordingly, the office links both classic intelligence and operational factions. CAWRO's proposed organizational structure reflects this dual role, in that its director is supported by deputies from both the intelligence community and the Joint Chiefs of Staff (Figure 5).

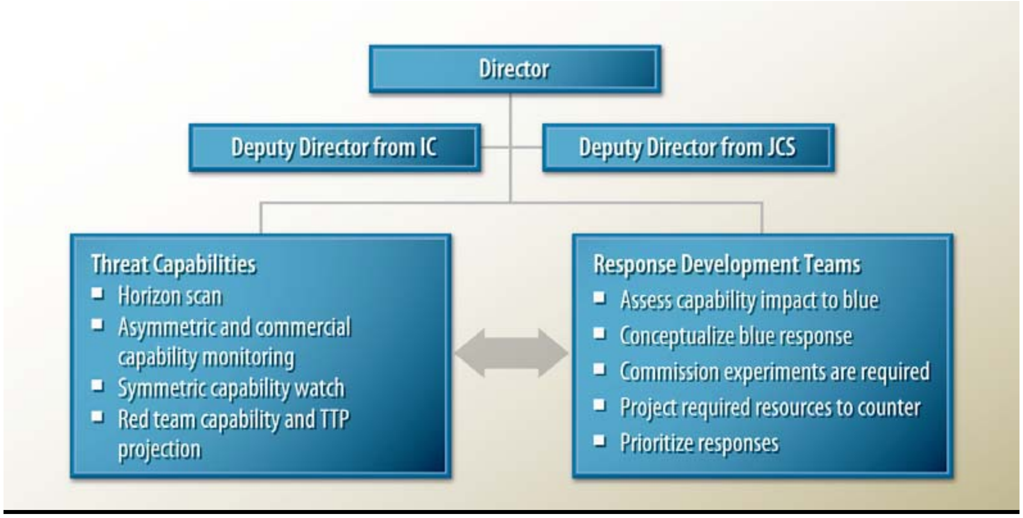

Director
Deputy Director from IC
Deputy Director from JCS
Threat Capabilities
Horizon scan
Asymmetric and commercial capability monitoring
Symmetric capability watch
Red team capability and TTP projection
Response Development Teams
Assess capability impact to blue
Conceptualize blue response
Commission experiments are required
Project required resources to counter
Prioritize responses

Figure 5. CAWRO Structure

The threat capability assessment function is responsible for scanning and sifting, capability projection, and providing input to net assessment. Response development teams, after defining and assessing response actions, produce the major output of the CAWRO, which is the decision package. A decision package includes options considered, priority, security impact, rough cost and schedule estimates, and a recommendation of organizations to be tasked. The set of possible action options is broad. They may include:

- Tasking the normal acquisition process to either create a new project or modify the key performance parameters (KPPs) of an ongoing system development
- Tasking a rapid fielding agency (see further discussion later in this chapter)
- Tasking the training and operational community to adopt new tactics, techniques, and procedures (TTPs) to address new capabilities
- Commissioning proactive measures to counter the postulated activity

Leadership and Staff

CAWRO's success depends on its people and their relationship to DOD's senior decision-makers. The CAWRO will likely produce findings and recommendations that will challenge or disrupt the mainstream and may not be readily accepted without top-level support. At the same time, the CAWRO is obligated to offer pragmatic ways to address shortfalls or gaps that it identifies.

Staffing such an organization must be done with care. Successful models include diverse, out-of-the-box, creative, and mutually supportive individuals, who can effectively communicate with mainstream DOD representatives, even while challenging mainstream thinking and assumptions. Much like DARPA, the CAWRO should be staffed by a small, permanent core that is supplemented by rotational staff from government, industry, laboratories, and academia.

CAWRO's leader is equally important. In addition to his or her trusted relationship with senior Department leadership and ability to harness a diverse group of bright, out-of-the-box individuals, he/she must be well networked to the technical and operational community(s) of government, academia, and industry to attract and motivate the "best and brightest" staff. Given the dynamic nature of the capabilities and responses, the CAWRO organization must be small, must be agile, and must avoid any semblance of bureaucratic behavior.

It is important to stress that the CAWRO is dealing with dynamic issues in a dynamic environment. Accordingly, CAWRO's budget needs to be set at a reliable level—sufficient for options exploration, evaluation, and prototyping, when needed—but flexible in expenditure. This approach will allow for the flexibility necessary to explore new threat spaces and properly assess Department response options.

Unique Characteristics

While many attributes of the CAWRO are similar in nature to existing DOD organizations, the concept as a whole is unique. A comparison to several existing organizations serves as an example. The CAWRO is similar to DARPA in that it may undertake prototyping. Its staffing philosophy is also similar. Unlike DARPA, it focuses on red capabilities and their potential impact on blue. In addition, it has a strong analytic arm that identifies vulnerabilities and considers fixes along the full doctrine, organization, training, material, leadership and education, personnel, and facilities (DOTMLPF) spectrum.

CAWRO is similar to the Office of Net Assessment in conducting red/blue assessments. Unlike this existing organization in the Office of the Secretary of Defense, the CAWRO links more closely to red teaming and undertakes prototyping. It not only conducts assessments, but also identifies and promotes solution options. The CAWRO is also co-mingled with strategic intelligence (indications and warning).

CAWRO will need to implement a scanning and shifting process like those being developed and used by the Director, Defense Research and Engineering, and the Office of Naval Research, but the scope should be broader to assess capabilities versus the science and technology emphasis of those efforts. (Ideally the CAWRO would utilize these activities as the starting point for its broader examination.)

Together these unique attributes enable the CAWRO to link together the entire cycle of surprise management and recommend actions directly to the Secretary of Defense. In conducting its mission, the CAWRO draws inputs from these and other organizations throughout the Department, as well as from academia, industry, and other government organizations.

RECOMMENDATION: INTEGRATION AND MANAGEMENT

The Secretary of Defense formally establish a Capability Assessment, Warning, and Response Office (CAWRO) to provide DOD senior leadership with timely assessment and warning of potential high-risk adversary capabilities, along with options for addressing them.

Red Teaming

Red teaming is the process that makes the outputs of red teams useful to decision-makers. It is a recognized need in many different contexts and has been recommended for increased use and attention by many groups, including the DSB in many reports over the last decade. Red teaming is underutilized within the Department of Defense. Red teams can fulfill various roles: playing the adversary, inventing plausible threats, challenging assumptions, serving as devil's advocate, and offering alternative approaches.

Red teaming is especially important in today's security environment. Nimble adversaries, with access to global technology markets, are very difficult targets for intelligence. Red teaming would serve important roles across DOD and help focus intelligence collection and analysis.

Despite its value, effective red teaming, especially above the tactical level, has proven difficult. The reasons are many. Red teaming can be threatening to many in an organization. The process must have consistent top-level support, but often does not, or worse, is remote from the decision-making process that it is intended to inform. Often the teams themselves are weak—lacking expertise, creativity, or appropriate "red" cultural backgrounds. In many cases, the red team is set up without the independence it needs to be effective and/or without the necessary interaction with “blue”—a critical element in determining capability gaps.

That said, good red teaming is possible—some existence proofs can be found in all of the military services. The Services’ tactical training regimes demonstrate the impact of effective red teaming. Pre-deployment training by the Army at Ft. Irwin and the Marines at 29 Palms includes realistic theater environments that place soldiers in Arabic speaking “villages” and cultures, complete with demonstrations, snipers, IEDs, bomb factories, and tunnels (Figure 6). Characteristics of these regimes include world-class red forces and open and honest critiques by commanders and subordinates alike.

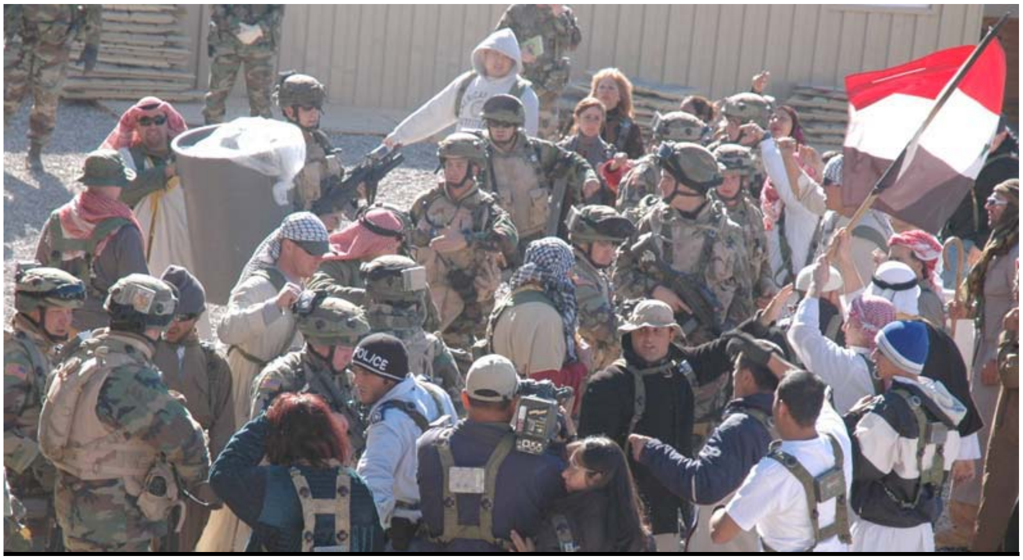


Figure 6. Pre-deployment Training at Ft. Irwin

While still a work in progress, Army leadership has directed a broader approach to red teaming based on growing demands from soldiers returning from deployments. Particular emphasis is being placed on supporting intelligence and command and control functions. A tiered training program has been established by U.S. Army Training and Doctrine Command (TRADOC) at Fort Leavenworth in which field grade officers are trained as red team leaders, both officers and enlisted are trained as members, and assignees to deploying units are provided “stop gap” training if more rigorously trained personnel are not available. Trained red teams are assigned to field commanders and report directly to the commander or his chief of staff.

The Navy submarine security program, in operation for over 35 years, offers another example—one of a program for critical strategic asset protection. This program is a model for ensuring that a mission of strategic importance to the Navy and the nation—namely the security of the strategic ballistic missile submarine force—is maintained against all known and technically feasible threats and technologies. The process involves continual assessment of threats to the strategic force, and how offensive (theirs) and defensive (ours) capabilities will interact. It focuses on the full range of technical and operational vulnerabilities over the long term (measured to date in decades). It is intimately partnered with intelligence, which serves roles as both the educator and the educated. Security boundaries for special access programs and intelligence information are removed for those involved in the program. It operates with a fenced and inviolate budget, is accountable to top-level leadership, and has strong governance. The results are a force more resilient in dealing with surprise, a force whose design and operations continuously evolve to account for what it learns, and maybe most important, an environment in which constructive self-assessment and improvement are the norm rather than the exception.

The general principles of the ballistic missile submarine model can be stated as follows:

- Examine what the nation’s adversaries know about the United States and how they know it.
- Identify U.S. vulnerabilities, regardless of adversary knowledge, and how they can be ameliorated.
- Define the near- and far-term consequences if “capabilities” migrate into the hands of adversaries.
- Identify specific adversary capabilities, and whether and how they are of value to the nation, to either exploit or to utilize.

One could imagine any number of strategically important functional and war fighting areas that could benefit from such continuous assessments in the context of capability surprise—areas such as cyber, other legs of the nuclear triad and associated infrastructure, space capabilities, Navy battle group survivability, air superiority, and many others.

Achieving a Red Teaming Culture

Red teaming has been recommended for many years in numerous ways, but has yet to become a cultural norm for DOD—especially in addressing strategic-level issues or as a part of major acquisitions or exercises. We focus here on recommendations that address the critical role of red teaming for successful surprise management, but red teaming is important in its own right. Regardless of the motivation and the clear benefits, red teaming will not become pervasive and persistent without sustained and aggressive leadership from the top.

The Secretary of Defense should direct the use of red teaming throughout DOD—in acquisition activities, exercises, experiments, planning, and strategy. The Secretary should task the Office of the Secretary of Defense (OSD), the combatant commands, and the Services—both the acquisition and operational communities—to develop, maintain, and apply red teaming best practices guides. Red teaming should be the subject of continuing intellectual activity in professional military education and other relevant institutions—the Army's effort at Fort Leavenworth serves as an example.

In addition, the Secretary should require more aggressive use of red teams in exercises, especially in addressing the "known" surprises involving adversary cyber, space, and weapons of mass destruction attacks. Operations should be pushed to failure or extremely degraded performance so that forces understand that such diminution of performance is possible and learn what to do about it. It is also essential to capture lessons learned and follow up to ensure they are applied. Failure to allow plausible red team attacks and demonstrate the consequences through exercises leads to a false sense of security and stifles initiatives that could redress vulnerabilities.

The Secretary of Defense should lead by example by establishing a strategic-level red team that can challenge national security and national military strategies. This small team of 5–6 individuals, augmented with other expertise as required, would report to the Deputy Secretary of Defense. This would be a continuing activity, meeting regularly with DOD top leadership, not just *ad-hoc* before a new strategy is issued. The group will be effective only if it maintains the strictest confidentiality and prevents "leaks." Staffing such a team with creative, forward-looking, and trusted individuals is particularly important.

Finally, red team products need to be "processed" to be useful to decision makers. Red teams can help anticipate capability and strategy surprises with which adversaries might confront the nation. But these products need to be linked to a process that illuminates the relative consequences and likelihood of potential threats, and facilitates decision-making about strategy, plans, programs, and intelligence collection. In other words, red teaming products need to be tied to all elements of surprise management, as described previously in this chapter on the mission and activities of the CAWRO.

Implementing these recommendations is a leadership and cultural challenge: to imbue throughout DOD a sense of responsibility for aggressive self-examination through continual challenge and commitment to make its programs and plans more robust. For it to be effective, red teaming must be taken to heart—not viewed simply as another box to check.

RECOMMENDATIONS: RED TEAMING

The Secretary of Defense direct the use of red teaming throughout DOD:

- All organizations develop and maintain red teaming best practice guides.
- Make red teaming the subject of continuing intellectual activity and professional military education and other relevant institutions.
- Require, with the Chairman, Joint Chiefs of Staff, more aggressive use of red teams in exercises and ensure retention and application of lessons learned.

The Secretary lead by example and establish a strategic-level red team to challenge and inform national security and top level defense policies and strategies[7]

The Office of the Secretary of Defense, combatant commands, and military services tie red-teaming products to all elements of surprise management.

Rapid Fielding

Mainstream DOD acquisition system and business processes are not well equipped either to anticipate or respond to urgent needs. They do not adequately meet challenges in a world that moves more quickly than a 10–20 year development cycle. Business processes, which include budgeting, requirements, and contracting processes, are risk-averse and were created to support long, complex development and production programs focused on very reliable, high-performance solutions. DOD's acquisition system was established and evolved over decades to produce sophisticated capabilities in a disciplined and controlled

[7] In fact, this has already happened, at least to a degree. Gen. James Mattis sent a memo in March 2009 to Defense Secretary Robert Gates calling for the creation of a Quadrennial Defense Review red team to examine defense planning scenarios tied to complex, hybrid threats. Secretary Gates has since established such a red team, which Mattis co-chairs.

set of processes. These processes also allow extensive transparency in the expenditure of public funds to ensure that legal and policy controls are met. But with these legal and fiscal demands comes a significant amount of oversight and checks and balances, which slow down the process.

Many past studies, including a number by the Defense Science Board,[8] have examined the DOD acquisition system and proposed numerous changes to improve the speed and agility of the system, either within the basic system itself or by providing an alternative path for those cases in which speed of response is more important than achieving a guaranteed “perfect” solution. The work of these studies will not be repeated here. Rather this study focuses on the ability of the Department to close serious capability gaps quickly, especially those that might result from recommendations of a CAWRO or red teaming activity. The study’s principle conclusion is that the major systems acquisition process was not designed to nor can it adequately address the kind of “on the edge” capabilities often called for in today’s security environment.

Yet, in many cases, the acquisition community has been successful in providing rapid solutions when an urgent priority or nature of the problem warranted. When a problem which demands a very quick response arises, DOD operational and acquisition managers are able to use—and have used—every means available to overcome bureaucratic barriers and solve the problem. These successes can be understood by those familiar with many successful “black” (classified) programs or some special materiel needs that arose during combat, such as occurred in Gulf War I. In cases where extraordinary measures were demanded, DOD has put focused leadership, funds, and skilled people on the mission to make it happen. However, in most cases, these successes did not occur within the “normal system,” but where leadership intervened to enable managers to act on the demand for rapid results by working “around” the normal system in all ways possible within the legal and regulatory restrictions.

In fact, numerous rapid reaction programs and organizations have arisen to respond to urgent needs as defined by combatant and component commanders. It is estimated that these programs have spent approximately $50 billion[9] over the period 2005–2009, and are staffed by several hundred people, mostly located in

[8] The two most recent of these are the *Report of the Defense Science Board on Creating a DOD Strategic Acquisition Platform*, April 2009, and *Report of the Defense Science Board Task Force on the Fulfillment of Urgent Operational Needs*, July 2009.

[9] This figure is dominated by the combination of Joint Improvised Explosive Device Defeat Organization (JIEDDO) and the Mine Resistant Ambush Protected vehicle program, which in combination represent approximately 80 percent of this expenditure.

OSD, although additional rapid fielding capabilities exist throughout the military services as well.

While typically successful in meeting the urgent need that creates them, these programs can create problems. They tend to be *ad-hoc* in formation and one-of-a-kind—such as creation of JIEDDO to focus on the improvised explosive device threat—with little emphasis on training and sustainment requirements associated with fielding. Since these organizations and programs are initially designed to be temporary, for the purpose of meeting a critical need, there is little effort to establish institutional memory and no process for "learning" or process improvement. The profusion of independent approaches by these organizations can be confusing to contractors and most are supported by funding drawn from the wartime supplement to the DOD budget. And no process exists to review the need for continuing the function after achieving its original purpose.

In spite of this workaround approach by the United States, today's adversaries are able to employ every means possible with whatever processes or discipline are required (or not required) to adapt or adopt technologies to target U.S. vulnerabilities—to adequate effect. Even adversaries with long and bureaucratic acquisition systems of their own can now more quickly adopt asymmetric capabilities to target U.S. weapon systems moving through DOD's ponderous acquisition cycle.

This combination of factors—the problems with the "one-off" approach for each special rapid fielding need, the rapid adaptation of adversaries, and the continued demand for urgent needs from the war fighter—suggests that a more consistent, rapid, and robust approach is needed when necessary, one in which exceptional, novel, and unusual solutions or extraordinary responsiveness can be achieved.

This study recommends that DOD create a standing Rapid Capability Fielding Office (RCFO) that reports directly to the Under Secretary of Defense for Acquisition, Technology, and Logistics. The principles of operation for such an organization should be as follows:

- It should operate with "colorless" money—allowing resources to be diverted to programs with the most urgent need as they arise.
- The organization should draw on successful attributes, including the somewhat unique culture of DARPA and the acquisition process in the Special Forces Command as organizational models, as well as build on lessons drawn from experiences in other rapid fielding efforts (both

positive and negative), such as the Mine Resistant Ambush Protected (MRAP) vehicles program.

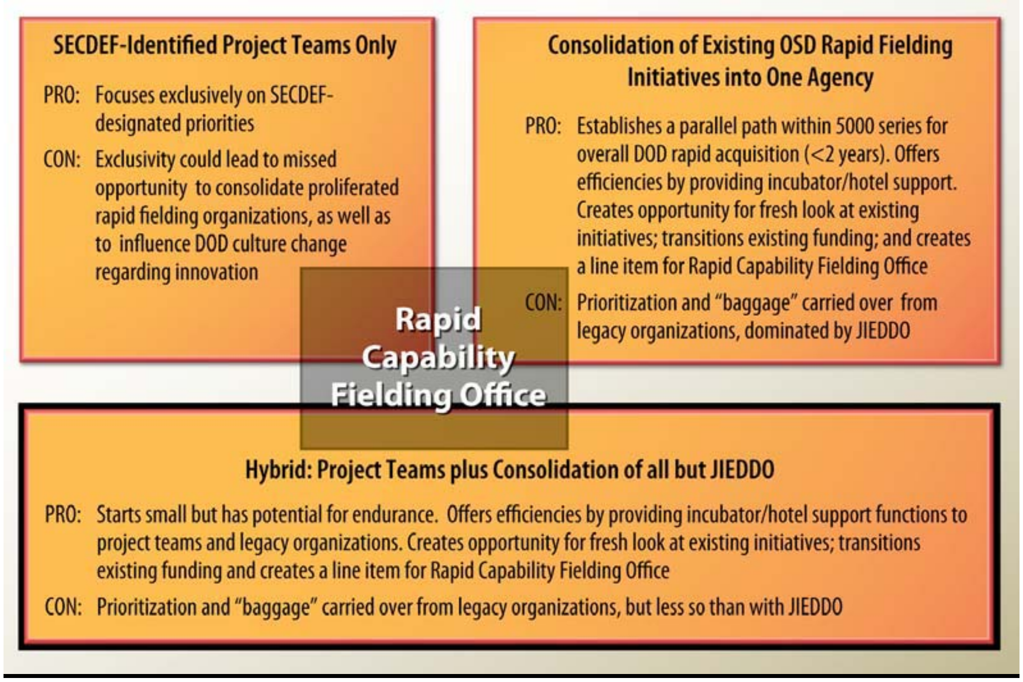
- The focus of the organization should be on rapid fielding, including, but not necessarily limited to, materiel acquisition of time-urgent capabilities. The nature of the needed capability may indeed require acquisition of new capability, but solutions that adapt existing capabilities or tactics, techniques, and procedures should also be part of the trade space.
- The staff should comprise a small group of exceptional people who would provide a core capability associated with start-up and support of new initiatives, have the ability to recruit project teams tailored to a given initiative, and ensure the dismantlement of those teams once their job is properly completed or transitioned to a Service or other pre-designated owner.
- Consolidated into this activity would be most of the existing OSD rapid fielding initiatives whose missions are still valid, except for JIEDDO.

Expanding on the above points, each project would be approved and chartered by the Secretary of Defense. A dedicated, expert project team would then be formed to carry out the project, with a predefined sunset. That is, once the team completes its mission, it would execute a transition, negotiated at the project's inception, to a lead military service or agency that would take on long-term sustainment responsibilities, if that is needed. Each team would implement a single, time-critical, priority fielding project and have goals focused on solving a specific challenge, without a predetermined solution. The teams would be staffed with exceptional, can-do people who would call on the expertise of mainstream service organizations—acquisition, logistics, operations and maintenance, training, and others—to execute projects. While a DARPA-type model is preferred, we assert that DARPA is not the correct organization to do this. This concept requires a different type of staff with emphasis on fielding, training, program planning, and management rather than the very different activities required for a focus on technology development.

The small core staff of typically 20 to 25 individuals would not only stand up each project team, but would also provide a core of enabling services including continued recruiting and staffing assistance, office space, contract management, budgeting, accounting, and routine administrative support. Institutional memory would reside with the permanent staff, along with the responsibility of disseminating lessons learned and best practices gained through each project.

Implementation

The RCFO can be implemented in a number of ways—and even within this study there were varying opinions as to what might work best (Figure 7). One option is an organization dedicated only to the Secretary of Defense's priorities, some of which might come from recommendations out of the surprise management process conducted by the CAWRO. This option has the advantage of limited tasking, and focuses the RCFO on only the highest priorities. The expectation here is that the Services would still have their own rapid-response organizations. The downside of this approach is that its exclusivity could lead to a missed opportunity to consolidate proliferated rapid fielding organizations in OSD, as well as to influence DOD culture change regarding innovation in fielding new capabilities.



SECDEF-Identified Project Teams Only

PRO: Focuses exclusively on SECDEF-designated priorities

CON: Exclusivity could lead to missed opportunity to consolidate proliferated rapid fielding organizations, as well as to influence DOD culture change regarding innovation

Consolidation of Existing OSD Rapid Fielding Initiatives into One Agency

PRO: Establishes a parallel path within 5000 series for overall DOD rapid acquisition (<2 years). Offers efficiencies by providing incubator/hotel support. Creates opportunity for fresh look at existing initiatives; transitions existing funding; and creates a line item for Rapid Capability Fielding Office

CON: Prioritization and "baggage" carried over from legacy organizations, dominated by JIEDDO

Rapid Capability Fielding Office

Hybrid: Project Teams plus Consolidation of all but JIEDDO

PRO: Starts small but has potential for endurance. Offers efficiencies by providing incubator/hotel support functions to project teams and legacy organizations. Creates opportunity for fresh look at existing initiatives; transitions existing funding and creates a line item for Rapid Capability Fielding Office

CON: Prioritization and "baggage" carried over from legacy organizations, but less so than with JIEDDO

Figure 7. Implementation Options for Rapid Capability Fielding Office

Another option would consolidate all the rapid acquisition offices, including the JIEDDO, into one agency in order to give RCFO adequate staff and budget to execute larger scale efforts. RCFO activities could be motivated by either the surprise management cycle or other military needs of any urgent nature. This approach establishes a parallel path within the 5000 series for overall DOD rapid acquisition (those acquisitions and fielding efforts completed in <2 years). It also offers efficiencies by providing incubator/hotel support. In addition, consolidation creates an opportunity for a fresh look at existing initiatives to determine whether they have a continued mission, transitions existing funding, and creates a line item for RCFO. Its downside is prioritization and the "baggage" that could be carried over from legacy organizations. Because of its size, JIEDDO would likely dominate the new organization, greatly influencing its operations.

A hybrid model, which many in the study believed to be the best path forward, would propose a consolidation of all but JIEDDO. This instantiation of the RCFO would give top priority to decisions for rapid fielding resulting from the surprise management cycle, but could also take on urgent needs that the Services were unable to handle. JIEDDO is focused on a particular set of issues that is expected to endure for some time; forcing it into the RCFO where the intent is to "sunset" activities creates a mission mismatch. This approach starts small but has potential for endurance. It offers efficiencies by providing incubator/hotel support functions to project teams and legacy organizations. The hybrid model also creates an opportunity for a fresh look at existing initiatives; transitions existing funding and creates a line item for a Rapid Capability Fielding Office. Like the other consolidation approach, "baggage" can be carried over from legacy organizations, but less so than with the inclusion of JIEDDO.

Regardless of the approach, flexibility will be critical to the RCFO's success. First, the RCFO must employ risk and contracting models differently than in normal programs. It will be important to cast a wide net for possible solutions if time allows—foreign, commercial, laboratories—and to fund requests for proposals quickly after initial screening and selection. The office will need to replace normal risk management concepts and payment policies with a higher level of risk taking; funds should be provided from day one. That said, the quality of the core staff and project teams must be such that their combined experience can serve to mitigate risks that are otherwise designed into the regulations that underlie the cumbersome mainstream process.

While large, traditional defense firms have scale and are savvy in DOD contracting and management demands, they may not have novel or unusual solutions that best address unique or "on the edge" surprise threats. Solutions to unusual challenges may often reside in small firms, independent laboratories, and other non-traditional defense providers. RCFO's rapid response teams must, therefore, be skilled in finding and dealing with both unconventional as well as conventional providers. Contracting approaches must be commensurate with compressed timeframes, using letter contracts to turn on projects and DARPA-like contracting approaches.

Exceptional steps must be taken to address manufacturing, training, and logistics support needs. It will be important to develop close working relationships with both users and suppliers—and to do so at the start of the process. This approach requires unique, high-trust relationships with industry, and vice versa. Because of the compressed timeframe for fielding, the normal sequence of production and logistics activities are highly compressed or overlapped. Initial field support should be funded to gain user acceptance until transitioned to a Service owner for the long term. It may be required to send a field training team for operations and support training upon initial deployment of solution to the war fighter. In some cases, there may also be a need to develop mechanisms for dealing with capital equipment, long lead, and surge production.

To avoid the large number of organizations that exist today, it is crucial to enforce the sunset clause for RCFO project teams. If the concepts for this organization are followed, as described above, it will not be difficult to dissolve the project teams once their mission is complete, as transition to an organization that will sustain the fielded solution will already have occurred. And resources from the RCFO can be targeted to the next urgent need identified.

Recommendation: Rapid Fielding

USD (AT&L) establish a standing Rapid Capability Fielding Office (RCFO) to improve DOD capabilities for addressing priority surprise capability gaps and supporting urgent war fighter needs. The office should:

- Report directly to the USD (AT&L)
- Operate on colorless money
- Consolidate most, if not all, existing OSD rapid fielding initiatives into one organization, except for JIEDDO
- Form dedicated expert project teams, with predefined sunset; each individual team:
  - implements a single, time-critical, priority acquisition and/or fielding project
  - is staffed with a small number of exceptional can-do people
  - has goals focused on solving a specific challenge
  - derives support from mainstream organizations as needed
  - up front plans for and negotiates transition of all ongoing efforts to lead Service with longer term responsibility
- Provide permanent core of enabling services

Strategic Intelligence

Intelligence underpins all elements of surprise management, as both a support and a supported function. In managing surprise, the intelligence community will be called upon to provide an understanding of adversary threat intentions and capabilities and to maintain current situational awareness through positive collection, analysis, and support.

The United States created a peacetime intelligence community in order to avoid surprise—the lessons of Pearl Harbor and the Soviet's rapid acquisition of nuclear weapons after WWII. The first line job of U.S. intelligence is to guard against surprise by identifying current as well as prospective threats. When surprise does occur and policy makers and operators must take action, intelligence supports national security decision-making and crisis management.

Creating difficulties for intelligence are adversaries who seek to inflict surprise by hiding and disguising what they are doing and misleading the nation about their plans, intentions, and capabilities. The more adversaries know about how U.S. intelligence works, the better they can design and employ deception and denial techniques. It is the job of U.S. counterintelligence to determine what and how adversaries know about the United States, in order to counter foreign intelligence threats and to inform security measures to protect essential national security secrets.

Intelligence organizations employ specialized quality controls to guard against being surprised themselves, some of which have atrophied and need reinvigoration. These include foreign denial and deception analysis ("red teaming" of U.S. analytic products) and strategic counterintelligence and operations to degrade foreign intelligence capabilities. The potential for strategic capability surprise gives rise to the need for a modern indications and warning process that can help flag emerging threats, and for well-developed protective security programs that take surprise into account and plan accordingly.

There are particular ways in which intelligence disciplines can support activities related to both creating and mitigating surprise. For the purpose of dealing with surprise, the study focused on two intelligence-related areas:

1. The issue of warning and ways the warning process can be made more effective for both intelligence and customers at the policy, technology, and operational levels
2. How the intelligence community could better identify and counter foreign denial and deception

Indications and Warning

The earlier that the nation can gain insights into an adversary's plans, intentions, and capabilities, the better are the chances that timely warning will be provided. This, in turn, provides increased opportunity to take measures to defeat or mitigate emerging and emergent threats. The nation needs a modern 21st century indications and warning (I&W) process focused on capability surprise. The CAWRO process, described previously, is responsible for its own warning-related activities, supported by horizon scanning of technically feasible threats. It requires warning of both traditional geo-political situations as well as threat data of global and adversary plans, intentions, and capabilities. This information needs to be augmented by intelligence warning assets to provide threat warning. Defining a relationship between the intelligence community I&W offices and the CAWRO can provide an enhanced environment for focusing on both technology and geo-political warning and threat horizon issues, and will be of net benefit to both the DOD surprise management and the intelligence community I&W processes.

The intelligence community has been struggling to implement its new I&W processes at the analytic level across the community. It would benefit both the I&W community and the CAWRO to have an intelligence warning cell resident within the CAWRO to inject warning information from the intelligence community. The intelligence warning community would develop more effective indication templates by participating in horizon scanning, net assessment, and red teaming. DOD would receive improved assessments of geo-political situations and threat data. To support all of this, the intelligence community should also take on the additional and specific mission of identifying adversary vulnerabilities that can be exploited for surprise and other purposes by the United States.

The intelligence community deputy leadership proposed for the CAWRO can serve to drive unique inter-relationships, mutual support, and a culture devoid of stovepipes. But even if the CAWRO is not established, a warning cell, such as proposed here, should still be placed within the office of the Under Secretary of Defense for Intelligence.

RECOMMENDATION: INDICATIONS AND WARNING

The Director of National Intelligence (DNI) Warning Office in the National Intelligence Council provide adequate resources for "strategic intelligence" and establish a cell within the CAWRO.

Denial and Deception

Adversaries seek to inflict surprise by hiding and disguising what they are doing, and by misleading the United States about their plans, capabilities, and intentions. There are numerous historic examples of this, as well as U.S. experiences in perpetrating its own forms of deception. Deception has played a major role in strategic surprise.

DOD understands and plans for military denial and deception at the tactical level, but presently there is no process to enable defense strategy to be informed by the potential for strategic denial and deception. Even the key judgments of the National Intelligence Estimates are not subject to denial and deception sensitivity analysis except when specific challenges arise—which are rare, unpopular, and *ad hoc*. Furthermore, programs and people to assess and counter foreign denial and deception have atrophied.

Accordingly, the Under Secretary of Defense for Intelligence, with support from the DNI's Foreign Denial and Deception Committee, should establish denial and deception teams in appropriate locations within the Department and the intelligence community—including at the level of net assessment and CAWRO activities to provide tools and processes to enhance the detection of denial and deception.

RECOMMENDATION: DENIAL AND DECEPTION

The Under Secretary of Defense for Intelligence establish teams in the intelligence community and Department of Defense, especially to support the CAWRO, to focus on detection of adversary denial and deception.

Chapter 5. Summary and Recommendations

It is time for the U.S. national security establishment to develop a healthy institutional paranoia: the nation must expect to be surprised and should be doing a better job of getting ready for it. Because of the globalization of knowledge and technology, and the ability of small groups without vast resources, visible infrastructure, or industrial capability to inflict great harm, the nation's leaders need to worry about capability surprise today much more than in the past. The challenges and losses the nation has been experiencing in operations in Iraq, Afghanistan, and elsewhere could turn into true destruction in the future due to proliferation of technology, and most worrisome, weapons of mass destruction.

Capability surprise has generally not resulted from pop-up technologies or intelligence failures, but from not acting on information already in hand. Intelligence, although still a vital component of avoiding, preparing for, and mitigating surprise, cannot alone provide a solution to dealing with surprise. Even in the seemingly more manageable bilateral world of the Cold War, the surprises the nation dealt with did not occur simply as result of intelligence failures. Deciding what to act upon and to what degree in today's complex world will be even more difficult than in the past, and will require mechanisms at the highest level of the Department that are not currently in place.

The increased attention called for in this study must be devoted to both "known surprises" as well as the "surprising surprises," albeit in different ways. For the former, the issue is a matter of getting serious about the handful of pressing threats where the evidence is clear, the potential damage huge, and actions to counter them inadequate to date. It is a matter of first being prepared to prevent these surprises and second to mitigate them to the extent possible should an incident occur. For surprising surprises, for which the evidence and potential consequences are less clear and the possibilities are many, the Secretary of Defense must institute a process—run by the right type of people and far-sighted leadership—to focus attention, take rapid action when and where it makes sense, and maintain the full support of the entire Department.

The biggest challenge for the Secretary in implementing the recommendations of this study will be to attain the support of the Department. Large bureaucratic institutions are generally threatened by self-criticism: questioning strategies, objectives, and methods; as well as different ways of doing things, particularly at the strategic level. To overcome this hurdle, DOD needs the following:

- An analysis component for dealing with surprise that gathers and assesses information, focuses intelligence collection, develops options, and presents them to the leadership
- A symbiotic relationship with long-range analysis and warning groups in the intelligence community
- A culture of aggressive red teaming, exercising, gaming, learning, self assessment, and improving
- A rapid action component structured and staffed to field effective remedies to surprise in weeks to months, not years to decades
- The discipline to continuously revisit assumptions, plans, and efforts—understanding that this is not a static game

Yet none of these capabilities can be achieved without leadership. In the end, the most important element in improving the Department's abilities to prevent capability surprise will be the leadership that the Secretary of Defense and his immediate subordinates display to the rest of the Department.

While this study has identified many shortfalls in DOD's ability to address surprise, it also discovered a number of building blocks that could provide the confidence that needed changes are possible. The foremost contributor will be the military leadership that is already transforming its thinking and approaches based on experiences gained in Operations Iraqi Freedom and Enduring Freedom. These conflicts have produced a cadre of uniformed leaders at all levels who deeply understand the value of challenging assumptions, looking at the world through many different lenses, and anticipating and dealing with surprise.

Other parts of DOD, most notably the science and technology and intelligence communities, are recognizing that old approaches no longer satisfy current needs. In several instances, new methodologies that are bringing these two communities together are being tested. In addition, each Service has examples of effective red teaming, largely at the tactical training level, where it is safe to self-critique and/or have junior service members point out the shortcomings of more senior decision-makers. OUSD (AT&L) has also recognized the need for effective rapid fielding. Through the Office of Technology Transition, OUSD (AT&L) has conducted its own self-assessment of existing organizations and is implementing a pilot program to test best practices.

With these capabilities as a starting point, the study looked to identify a few actions that would significantly change and improve the Department's ability to address surprise. These key recommendations are summarized in the remainder of this chapter.

Recommendations

RECOMMENDATION: INTEGRATION AND MANAGEMENT

The Secretary of Defense formally establish a Capability Assessment, Warning, and Response Office (CAWRO) to provide DOD senior leadership with timely assessment and warning of potentially high-risk adversary capabilities, with options for addressing them.

The elements of surprise management are unlikely to achieve their potential impact, even if perfected, without some function that integrates and guides them. The Defense Science Board is normally reluctant to recommend creating new organizations, but in this case, the Board feels that it is critical to the success of managing surprise. Such an organization must have:

- High level reporting and accountability
- Truly “best and brightest” talent that is able to effectively challenge the mainstream
- A leader who commands the respect of both Department leadership and his or her staff
- Close coupling to the intelligence, red teaming, experimentation, and acquisition communities

RECOMMENDATION: RED TEAMING

The Secretary of Defense direct the use of red teaming throughout DOD:

- All organizations develop and maintain red teaming best practice guides
- Make red teaming the subject of continuing intellectual activity and professional military education and other relevant institutions
- Require, with the Chairman, Joint Chiefs of Staff, more aggressive use of red teams in exercises and ensure application of lessons learned

The Secretary of Defense lead by example and establish a strategic-level red team to challenge and inform national security and defense policies and strategies

The Office of the Secretary of Defense, combatant commands, and military services tie red-teaming products to all elements of surprise management

The Department needs to make red teaming ubiquitous. Overcoming the discomfort (for some) and threat (for many more) of self-criticism that ubiquitous red teaming would introduce requires strong and sustained leadership at the top of the Department. Not only should a number of steps be directed by the Secretary of Defense, as detailed in this recommendation, but he should also lead by example. The Secretary should establish a "strategic" red team charged with challenging national security and high-level military strategies. In other words, posit what others will do in response to U.S. policies and doctrine that might be unexpected or undesired.

Should the study team's vision of pervasive red teaming be realized, it will generate a rich set of products that should continuously inform and be informed by the surprise management cycle.

RECOMMENDATION: RAPID FIELDING

The Under Secretary of Defense for Acquisition, Technology, and Logistics establish a standing Rapid Capability Fielding Office (RCFO) to improve DOD capabilities for addressing priority surprise capability gaps and supporting urgent war fighter needs. The office should:

- Report directly to the USD (AT&L)
- Operate on colorless money
- Consolidate most, if not all, existing OSD rapid fielding initiatives into one organization, except for JIEDDO
- Form dedicated expert project teams, with predefined sunset; each individual team:
  - implements a single, time-critical, priority acquisition and/or fielding project
  - is staffed with a small number of exceptional can-do people
  - has goals focused on solving a specific challenge
  - derives support from mainstream organizations as needed
  - up front plans for and negotiates transition of all ongoing efforts to lead Service with longer term responsibility
- Provide permanent core of enabling services

The study team proposed varying options about what organizations should be consolidated into this rapid fielding office. We present the prevailing option here, but regardless of what option might be adopted, the normal practice of establishing *ad hoc* organizations in response to individual urgent war fighter needs or pop-up surprises will not result in an effective capability within the Department. It appears that the Department recognizes the need to "clean up the mess" of the many existing organization and is already taking steps at a pilot level to create a more robust innovation process. The success of any changes, however, depends on the discipline of leadership in the RCFO to create effective project teams for the task at hand and then dissolve those teams once their mission is performed.

RECOMMENDATION: STRATEGIC INTELLIGENCE

The DNI Warning Office, in the National Intelligence Council, provide adequate resources for "strategic intelligence" and establish a cell within the CAWRO.

The Under Secretary of Defense for Intelligence establish teams in the intelligence community and Department of Defense especially to support the CAWRO, to focus on detection of adversary denial and deception.

Whether all or part of the recommendations of this study are acted upon, two important functions of the intelligence community must be strengthened in order to support any aspect of surprise management. One is to greatly improve "strategic" intelligence that monitors adversary intent and capabilities over time and continuously updates key adversary vulnerabilities that the nation can exploit. Aspects of this function should also exist within the CAWRO. The second is in the area of detecting foreign denial and deception, which effectively constitutes red teaming within the intelligence community.

RECOMMENDATION: KNOWN SURPRISES

The Secretary of Defense establish a formal mechanism to ensure Department progress in addressing the limited number of most critical threats—the known surprises. The Secretary direct:

- CAWRO to conduct an ongoing assessment of the risks posed by these known surprises: foreign capabilities, U.S. strengths and vulnerabilities, and net potential consequences

- Services and appropriate combatant commands to perform a series of operational exercises, games, and red teaming activities that both inform and reflect the risk assessment activity above
- USD (AT&L) and Chairman, Joint Chiefs of Staff, identify a series of measurable goals and time frames for improving U.S. abilities to deter; fight through; detect, prevent, and mitigate; use appropriate offensive measures

The Secretary of Defense and Chairman, Joint Chiefs of Staff, engage and educate congressional leadership on these issues.

The Secretary of Defense must take the lead in addressing known surprises—to deal with these threats before they actually do become surprises. The CAWRO can be effectively used to assess these threats as well as the surprising surprises. In addition, the Secretary must make it clear by directive that the Department is going to fully understand the risks and opportunities in these areas and establish appropriate actions, plans, and schedules for mitigating the former and exploiting the latter. Equally important is the need to engage Congress in understanding these issues and the need to address them, and in providing the resources required to deal with them. In the end, dealing with known surprises requires the same leadership as dealing with the surprising surprises, beginning with the Secretary of Defense.

The Essential Requirement for Leadership

A recurring theme of this study is the critical need for leadership at the highest levels of the Department if the nation is going to be successful in anticipating, preparing for, rapidly countering, mitigating the effects of, and rebounding from strategic and/or existential surprise.

This report has outlined a number of specific recommendations focused on being prepared to counter or to fight through those very serious capability threats that are highly probable and that should not be a surprise if and when they do occur. It has also offered a systematic mechanism for sorting through the many other potential surprises—the surprising surprises—in a manner that allows the Department to develop and implement an affordable hedge strategy and the ability to react quickly if and when the need arises. But none of these recommendations will have a lasting effect, even if initially implemented, if the Department's senior leadership do not set an example for the rest of the institution to see.

In the view of this study team, the Department's leadership must display four essential elements both within DOD and to cross-agency teams:

- Encourage alternative viewpoints, some of which challenge the status quo.
- Require broad risk/opportunity assessment across a wide range of alternatives.
- Integrate and synthesize from a range of inputs and approaches—from "lessons learned" to innovation.
- Enhance knowledge through cross-domain teaming with shared accountabilities and recognition.

All of these elements share the same characteristics: they are obvious, they are easy to articulate, and they are difficult to do. If the nation is to prepare itself for the surprise challenges of the 21st century, it will be essential to do more than pay lip service to these needs. It will be up to the leadership within DOD to show by example and lead the nation to success.

Appendix A. Wicked Problems

One analytical framework that can help the Department of Defense anticipate and prepare for capability surprise deconstructs and examines “wicked problems,” which are complex, multivariable, and have no set solutions. This appendix will give an overview of wicked problems, some guidelines on their analysis, suggested applications, and case studies.

Definition of a Wicked Problem

A “wicked problem” is a construct devised by academic theorists Horst Wittel and Melvin Webber (Wittel and Webber 1973). Wicked problems are highly complex, wide-ranging problems that have no definitive formulation, are substantially without precedent, and have no set solution. They are frequently entwined in other problems and contain contradictory or incomplete data. Wicked problems involve many stakeholders with competing viewpoints and goals. Attempts to solve these problems impact other issues, and solutions can simultaneously contain positive and negative results. Solutions to wicked problems are themselves complex. There is frequently no one identifiable solution for the multivariate problems. The search for solutions never stops; every implemented solution has consequences for the other aspects of the problems, making measuring effectiveness difficult, if not impossible. The solutions sets are not finite and there is no well-described or well-defined protocol of permissible operations.

A wide range of problem solvers utilize the wicked problems construct as part of their analytical toolkit. Social scientists examine disparate issues such as the global war on terror or public health issues. Systems engineers utilize this construct when developing large enterprise level systems (Gharahedaghi 1999). Strategic capability surprise is a specific type of wicked problem.

Addressing Wicked Problems

Conventional linear thinking will arrive at less than complete or comprehensive conclusions when dealing with capability surprise. In an analysis of cognitive bias with regard to China policy, Josh Kerbel lays out principles to counter linear bias and mind-set (Kerbel 2004). According to Kerbel, an organization should:

- Culturally embrace uncertainty

- Emphasize the understanding of possibilities, not prediction
- Utilize alternative scenarios/futures regularly as a methodological approach to problem-solving
- Emphasize the explanation of the assumptions, key variables, and signposts for each scenario
- Resist the temptation to minimize analytical uncertainty by eliminating caveats
- Try to avoid picking a single result in the face of significant uncertainty
- Recognize that language both reflects and reinforces bias/mind-set and consciously adopt more non-linear terminology and metaphors
- Require all involved in the analysis to take a course in linear/non-linear thinking and dynamics
- Make a concerted and serious effort to pursue the development of agent-based modeling, visualization, simulation and other advanced computer tools and techniques for exploring and explaining the dynamics of highly complex and non-linear systems

Application within the Department of Defense

In previous periods where "surprise" was considered unacceptable, the Department reacted with alacrity, speed, and commitment. During these times, the DOD had:

- Concerted, long-term, senior-level commitment
- Oversight and responsibility vested in the most senior operating authority
- Dedicated and protected resources
- A professional, sustained cadre of personnel augmented by rotational personnel from the operational, technical, and intelligence communities
- Unique security arrangements that created an extraordinary level of protection for the activities, while at the same time within the activity eliminating all barriers to cross access to the security disciplines of the participants
- Continuous measure/counter measure deliberation:
  - exhaustive effort to understand what the adversaries know about the United States and how they know it

- identification of U.S. vulnerabilities, regardless of adversary knowledge, and a process to ameliorate those issues
- analysis of the consequences of all U.S. capabilities being placed at the disposal of the adversaries
- knowledge of adversary current and future capabilities, their implications for U.S. security and the value of incorporation of those capabilities into our systems, tactics, and policies

In examining and preventing capability surprise for the DOD today, three shifts in the early 21st century merit attention:

1. Technology and the operational application of capabilities move across borders at accelerated speed in the information age. A breakthrough new development is globally accessible within a greatly compressed time period.
2. Knowledge of U.S. systems, vulnerabilities, predispositions, and objectives is more accurate, readily available, and pervasive than at any previous time.
3. The number and diversity of potential adversaries have expanded dramatically. Where in the past only a small number of international forces could inflict serious harm on the country or its international interests, a large number of potential adversaries can now cause egregious damage to U.S. national security.

For many decades, the DOD has sustained an aggressive combination of technology, operations, and policy initiatives to keep the nation secure. These expanding threats and limited resources demand that the Department be managed with a combination of the best possible intelligence, the most aggressive technology programs, and inventive operational applications. There is benefit in an explicit methodology to highlight opportunities for interdiction and/or misdirection.

One option is to have a high-level, centralized organization be responsible for preventing or mitigating surprise, as recommended in the main body of this report. A central organization could ensure a reasonably exhaustive, capability-by-capability evaluation of the likelihood that an adversary will achieve a symmetric capability at parity with, or beyond our own; and the likelihood that an adversary can counter/deny us a critical capability. A central organization can have all the access required to understand present and future military capabilities while still ensuring the secrecy and sanctity of our development and operation of these critical capabilities. An organization that stands above the individual capability developers and maintainers can bridge across them and consider alternative courses of action that might hedge a capability in one modality with a capability or basket of capabilities across other modalities. And, an organization so-placed can actually manage the hedging process.

Case Study in Wicked Problems in the Intelligence Community

The U.S. intelligence community must continually deal with nonlinear variables, their implications, and constant change. One focus has been attempting to predict trends and policies within the Chinese government and military. Three perennial wicked questions involve China's political stability, its evolving role on the world stage, and its military capabilities and force structure. According to the article by Kerbel, the intelligence community's major problem in predicting Chinese behavior has been the following:

- Oversimplification—The debate on granting China normal trade relations in the 1990s centered on economic issues. Policymakers did not take into account the security and human rights issues that could have further instructed the U.S. decision to drop tariffs.
- Not realizing the inevitability of unintended consequences—China's entry into the World Trade Organization is again not just an economic event, but will have social, political, and economic effects for years to come. This action could cause "rising unemployment and demands for political change, on one hand, and the assertion that the World Trade Organization (WTO) will lead to exactly the opposite: extension of the political status quo because WTO-spurred economic growth will give the current regime greater legitimacy."
- Wicked problems cannot be repeated—Comparing China to the USSR leads to false analogies for analysts.
- Timing cannot be predicted due to unpredictable inputs and outputs—The Kuomintang (KMT) ruled Taiwan for fifty years, navigating the island's balance as an independent entity with China's insistence that it was part of greater China. Though many had predicted political reordering through the years, it was not until 2000 that the KMT lost its majority rule to the People First Party.

Case Study in Wicked Problem Solving in the Private Sector

Successful publicly traded companies are examples of agile organizations that can successfully navigate wicked problems. Because such companies seek to increase value for their shareholders and their shareholders traditionally give the companies' leadership great latitude for quick changes in strategy and execution, they are structurally better-positioned to tolerate greater risks and apply creative, nonlinear, open-ended solutions to their wicked problems. Shareholders, via their board proxies, can quickly punish poor decisions and wrong turns in this process via changes in leadership and demands for immediate strategy changes. Wal-Mart offers an example of a wicked problem and two approaches that it took (Camillus 2008).

For almost fifty years, Wal-Mart has been enormously successful at increasing market share via low-cost sourcing and using loss-leaders in their merchandise inventory to eliminate competitors (at which time, they can raise the prices to market level). However, Wal-Mart's wicked problem is that they have saturated their target market, yet must continue to show their shareholders ever increasing value. In addition, all their movements affect differing stakeholders, including employees, trade unions, investors, creditors, suppliers, governments, and others, sometimes creating their own wicked problems (law suits and negative publicity about human resource abuses are recent examples). From the myriad of options available to address the wicked problem of shareholder growth in an almost fully saturated market, two examples emerge.

The first example of wicked problem-solving is to try to sell different products in the existing American market. Since Wal-Mart has saturated the suburban and rural markets with low-cost items, it has attempted to modify its value proposition by stocking some upscale products and developing a brand persona that warrants higher prices. By taking this tactic, Wal-Mart is taking the strategy of one of its main competitors, Costco, which regularly stocks mid to upscale items in a discount setting. Initial indications are that this strategy is failing (Barbaro 2007). As with many attempted answers to wicked problems, Wal-Mart could not have anticipated the unintended consequences, namely that consumers devalued the upscale items and viewed them as cheap because they were in the Wal-Mart setting. Wal-Mart has now pulled back on stocking upscale items and is pursuing the higher price-point strategy via its introduction of organic foods.

Second, as part of a greater strategy to expand internationally, Wal-Mart has found a way to enter into India, which has particularly wicked, market-entry problems. India possesses laws that prohibit foreign companies from operating multi-brand retail outlets in the country. Wal-Mart responded by developing cash and carry wholesale stores for local retailers in a joint venture with Bharti Enterprises, an Indian telecommunications company. Characteristic of the wicked problem, a number of other wicked problems arise from this strategy: Wal-Mart must now work with the Indian government and within the Indian consumer products sector to build its supply chain. Additionally, if and when India's laws change, Wal-Mart will have to compete with the retailers that it supplies. These and other problems typify a business's challenges when confronted by non-linear strategic issues.

This cursory look at a business example can be replicated many times in the worlds of military, economic, political or operational capabilities. Wal-Mart's continually shifting approaches to its wicked problems exemplifies any organization's attempt to address nonlinear problems.

Summary

Wicked problems will characterize more and more of DOD's future challenges. This appendix has attempted to introduce the reader to the nature of such problems. There is a growing discipline of scientific investigation and management application in this area that DOD should become more aware of and begin to participant in. The interdependencies, complexities, and non-linear behavior of the modern world require something beyond the traditional approaches that were effective in a simpler time.

Works Cited

Barbaro, Michael. *International Herald Tribune*. March 2, 2007.
http://www.iht.com/articles/2007/03/01/business/walmart.php
(accessed August 30, 2008).

Camillus, John. "Strategy as a Wicked Problem." *Harvard Business Review*,
May 2008.

Gharahedaghi, Jamshid. Systems Thinking—Managing Chaos and Complexity:
A Platform for Designing Business Architecture. Burlington: Butterworth
Heinemann, 1999.

Kerbel, Josh. "Thinking Straight: Cognitive Bias in the US Debate Over China."
Studies in Intelligence, 2004.

"Leaked Memo Suggests Wal-Mart's Upscale Strategy May be Backfiring."
May 31, 2007. (accessed August 2008).

Wittel, Horst, and Melvin Webber. "Dilemmas in a General Theory of Planning."
Policy Sciences, 1973.

Terms of Reference

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

MAY 15 2008

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board (DSB) 2008 Summer Study on Capability Surprise

The United States (U.S) is in a never-ending race to maintain a capability edge against potential opponents. Despite significant U.S. science and technology prowess, numerous paths exist for adversaries to achieve "capability surprise." Many of the alternative paths for adversary capability development do not rely on leading edge science and are sometimes achieved at a significant cost advantage over U.S. capabilities. Fortunately, capability development paths exist without using cutting edge science and technology for the U.S. and may also create opportunities for the U.S. to employ cost imposing strategies on adversaries.

There are three different scenarios in which capability surprise can occur:

1. Surprise in the laboratory. Although less likely than some other forms of surprise due to the extensive intellectual interchange and competition among laboratory scientists, surprise from a fundamental scientific breakthrough is still possible. Breakthroughs in mathematics, algorithms, cryptography, and device technology, for example, can spring from anywhere. More likely are the surprises that might result from the clever first application(s) of scientific discoveries.

2. Surprise during transition from concept to fielded product. Transition time is affected by numerous issues, including: bureaucratic process, manufacturing capability, training, and logistics. Presuming we all share the same worldwide base of science, whoever can move it into fielded weapons systems the fastest has a real advantage – and some countries have the resources, agility, and will to accomplish this. An adversary that cares less about process, cost, and potential abuse and more about speed has the potential to get capabilities to the field more rapidly than we might expect, Furthermore, the spread of manufacturing technology, service and process improvement techniques, and management knowledge make the transformation of laboratory knowledge into reliable, repeatable, deliverable, maintainable equipment more likely. Globalization accelerates market workforce training and will accelerate the development of this capability as other countries compete in the global market.

3. Surprise introduced by the unconventional or unforeseen use of an existing capability. It might be commercial (e.g., the Internet as a command and control net) or a weapons system (e.g., the B-52 in a tactical support role). Innovative development of new capability using existing force structure can be extremely rapid, prove costly in combat, and be extremely effective. Another facet of this particular surprise mechanism is the employment of old or low technology against high-end U.S. capability.

Underlying the kinds of surprise are the reasons why surprise may occur. A partial list of such reasons includes:

a. Failure to respond to the introduction of a new capability
b. Planned response proceeds at too leisurely a pace
c. Failure to imagine a capability
d. Underestimating an adversary's prowess to introduce a capability
e. Assuming that an adversary would not dare to do such a thing

The study should focus on the *whats* and *whys* of capability surprise and the measures to ensure that DoD and its interested partners are best positioned to prevent, or mitigate, capability surprise against itself. It should assess the surprise mechanisms, dealing with how surprise may occur, and develop relevant recommendations in two domains: how to reduce the potential for surprise across the dimensions outlined above; and given that some surprise will always occur, how to better prepare ourselves to respond appropriately. Recommendations should also be formulated for ensuring that the Department, in coordination with the intelligence community, has both the people and processes in place not only to identify potential surprises across the dimensions outlined above but also, on an annual basis, to formally assess both risks and opportunities in dealing with them.

Finally, the study should assess cost-imposing strategies to include what adversaries may do to the U.S. and what the U.S. could do against potential adversaries, both with respect to high-end technology solutions and employment of low-end or old technology solutions. As part of this assessment, the study should also consider how the U.S. might impose surprise on its adversaries in rapid, cost effective, and unique ways.

The study will be co-sponsored by the Under Secretary of Defense for Acquisition, Technology and Logistics, the Under Secretary of Defense for Intelligence, the Vice Chairman of the Joint Chiefs of Staff, and the Commander, Joint Forces Command. Dr. Miriam John and Mr. Robert Stein will serve as Chairpersons of the Summer Study. Mr. R.C. Porter of OUSD(I) and Mr. Robert Baker of the Office of the Director of Defense Research and Engineering will serve as co-Executive Secretaries; and Lieutenant Colonel Chad Lominac, USAF, will serve as the DSB Secretariat Representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the “Federal Advisory Committee Act,” and DoD Directive 5105.4, the “DoD Federal Advisory Committee Management Program.” It is not anticipated that this Task Force will need to go into any “particular matters“ within the meaning of section 208 of title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.

John J. Young, Jr.

Study Membership

NAME	AFFILIATION
Chairs	
Miriam John	Private Consultant
Robert Stein	Private Consultant
Executive Secretaries	
Bob Baker	OSD/DDR&E
R.C. Porter	OSD/USD (I)
Senior Advisors	
Craig Fields	Private Consultant
John Foster	Private Consultant
Ted Gold	Private Consultant
George Heilmeier	Private Consultant
Bill Schneider	International Planning Services, Inc.
Vincent Vitto	Private Consultant
Challenge Panel	
Chair	
Gerry Yonas	Sandia National Laboratories
Members	
Bob Atkins	MIT
Roy Evan	MITRE
John Foster	Private Consultant
Rich Haver	Northrop Grumman Corp.
Ron Kerber	Private Consultant
Larry Lynn	Private Consultant
Joe Markowitz	Private Consultant
Jason Webster	Northrop Grumman Corp.
Institutional Process Change Panel	
Chair	
Joseph Braddock	The Potomac Foundation
Members	
George Cybenko	Dartmouth University
Bruce Deal	SET Corporation
Jacques Gansler	University of Maryland
Ted Gold	Private Consultant
Michelle Van Cleave	NDU
Technology Panel	
Chairs	
Zach Lemnios	MIT Lincoln Laboratory
Jim Shields	Draper Laboratory

NAME	AFFILIATION
Members	
Melissa Choi	MIT Lincoln Laboratory
Frank Fernandez	Private Consultant
Jim Gosler	Sandia National Laboratories
Anil Jain	Michigan State University
Steve Kornguth	University of Texas at Austin
Mark Lister	StratTechs, Inc.
Len Polizzotto	Draper Laboratory
Robert Popp	National Security Innovations, Inc.
Ron Sega	Colorado State University
Ann Marie Skalka	Fox Chase Cancer Center
Robert Tenney	BAE
Jim Thomas	Applied Minds, Inc.
Joe Walkush	SAIC
David Whelan	The Boeing Company
Government Advisors	
Jack Bell	L&MR
Mel Currie	NSA
Matt Hosey	NGA
Steve Thompson	DIA
Operations Panel	
Chairs	
Michael Hagee	Private Consultant
James McCarthy	USAFA/DFPS
Members	
Eric Evans	MIT Lincoln Laboratory
Greg Gardner	Oracle Corporation
Thomas Hammes	Private Consultant
John Hanley	Institute for Defense Analyses
John Hawley	Near Space Systems, Inc.
David Johnson	RAND Corporation
Jim Kurtz	Institute for Defense Analyses
James Lacey	Institute for Defense Analyses
Dawn Meyerreicks	Private Consultant
Dave Nichols	Private Consultant
Ron Sega	Colorado State University
Thomas Steffens	FLIR Systems Inc.
Bill Studeman	Private Consultant
Patrick Toohey	Sullivan Haave Associates
John Vines	Private Consultant
Linton Wells	National Defense University

NAME	AFFILIATION
Government Advisors	
R.C. Porter	OSD/USD (I)
Andrew Roberts	DIA
Transition and Fielding Panel	
Chairs	
Christine Fisher	Private Consultant
Bill Howard	Private Consultant
Members	
Dave Drumheller	ONR
Regina Dugan	Dugan Ventures
Ed Franklin	Raytheon
Matt Ganz	Phantom Works
Jan Herring	Herring and Associates LLC
Frank Kendall	Private Consultant and Attorney at Law
Ira Kuhn	Directed Technologies, Inc.
Bob Lucky	Private Consultant
Robin Murphy	Texas A&M University
Harry Raduege	Deloitte and Touche LLP
Joseph Santarelli	Booz Allen Hamilton
Leigh Warner	Private Consultant
Government Advisors	
Mark Mandeles	RRTO/Emerging Capabilities Division
Additional Government Advisors	
Russell Buttram	USMC Strategic Initiatives Group
Daniel Flynn	ODNI
Garth Jensen	OPNAV N81
Chuck Kimzey	U.S. Pacific Command
Don Wurzel	Arete Associates
Cecelia Phan	Joint Staff J6CTO
Steve Smith	HDQA G-3/5/7
Randy Tebbing	OUSD (I) CAMM
DSB Representatives	
Brian Hughes	DSB Executive Director
Charles Lominac	U.S. Air Force Military Assistant
Karen Walters	U.S. Army Military Assistant

NAME	AFFILIATION
Staff	
Barbara Bicksler	Strategic Analysis, Inc.
Rebecca Bortnick	Strategic Analysis, Inc.
Greg Byerly	Strategic Analysis, Inc.
Tim Cullen	Strategic Analysis, Inc.
Kelly Frere	Strategic Analysis, Inc.
John Fricas	Strategic Analysis, Inc.
Marcus Hawkins	Strategic Analysis, Inc.
Amy Hoang-Wrona	Strategic Analysis, Inc.
Jennifer Howell	Strategic Analysis, Inc.
Brian Keller	Strategic Analysis, Inc.
Teresa Kidwell	Strategic Analysis, Inc.
Toni Marechaux	Strategic Analysis, Inc.
Diane O’Neill	Strategic Analysis, Inc.
Ted Stump	Strategic Analysis, Inc.

Presentations to the Study

NAME	TOPIC
Plenary Sessions	
April 29, 2008	
Mr. Jeff Green Office of General Counsel, Office of the Secretary of Defense	Standards of Conduct
Mr. Ben Riley Director, Rapid Reaction Technology Office of the Director, Defense Research and Engineering (DDR&E)	Defense Policy Implications of Global Technology Trends
Mr. Andy Marshall Director, Net Assessment	Discussion on Capability Surprise
May 1, 2008	
Gen James Cartwright, U.S. Marine Corps Vice Chairman, Joint Chiefs of Staff	Discussion
Dr. Steve Chiabotti and Dr. Everett Dolman School of Advanced Air and Space Study, Maxwell Air Force Base	Theory of Capability Surprise
Mr. Larry Burgess Deputy Under Secretary of Defense for Collection and Analysis Mission Management	Discussion
May 19, 2008	
Staff, Central Intelligence Agency	Intelligence and Science and Technology Perspectives
Mr. Al Shaffer Principal Deputy Director of Defense Research and Engineering, Office of the Secretary of Defense	DDR&E Perspectives
Mr. Dan Flynn Deputy Director of National Intelligence for Analysis	Analysis Perspectives
May 21, 2008	
Mr. James Johnson Program Analysis and Evaluation, Office of the Secretary of Defense	Shaping the Pacific Region
Dr. Thomas G. Mahnken Office of the Under Secretary of Defense for Policy	Discussion

NAME	TOPIC
June 10, 2008	
Mr. Adam Nucci DDR&E	Global Emerging Technologies Study
Mr. Art Zuehlke Defense Intelligence Agency	Defense Intelligence Agency Perspective
Dr. Ruth David ANSER	Avoiding Surprise in an Era of Global Technology Advances
June 12, 2008	
Dr. Melissa Flagg	ONR Global
Mr. Chris Bannon	Navy Deep Red
Mr. George Spix	Microsoft Experience
June 25, 2008	
Dr. Anita Jones Former DDR&E	Information Technology Capabilities
Dr. Tony Tether Director, Defense Advanced Research Projects Agency (DARPA)	DARPA Perspectives
Mr. Christopher Darby CEO In-Q-Tel	Discussions
LTG John R. Wood, USA Deputy Commander, Joint Forces Command	Joint Forces Command Perspectives
Dr. Dave Johnson, RAND and Mr. Jim Lacey, IDA	Discussions
June 26, 2008	
General Anthony Zinni, USMC (Ret) and Ambassador Richard Armitage	Discussions
June 27, 2008	
Ambassador Kenneth Brill Director, National Counter-proliferation Center (NCPC)	NCPC Perspectives
LTG Thomas Metz, USA Director, Joint Improvised Explosive Device Defeat Organization (JIEDDO)	JIEDDO Perspectives
Dr. Don Kerr Deputy Director of National Intelligence	Discussions
July 22, 2008	
Dr. Jim Heath National Security Agency (NSA) Science Advisor	NSA Perspective

NAME	TOPIC
Mr. Frank Cappuccio	Lockheed Martin Skunk Works
July 23, 2008	
Andy Nicholson Senior Programme Leader, Dstl Farnborough, UK	An Allied Perspective
July 24, 2008	
Mr. Nick Marsella Co-Director, U.S. Army University of Foreign Military and Cultural Studies	Army Red Teaming
Dr. James Tegnelia Director, Defense Threat Reduction Agency	Discussion
Mr. Mike Leiter Director, National Counterterrorism Center (NCTC)	NCTC Perspective
Operations Panel	
May 2, 2008	
VADM Dave Nichols	Master 4GW Brief
July 23, 2008	
Frederick Brosk Office of the Under Secretary of Defense for Intelligence	Capability Surprise
Technology Panel	
June 26, 2008	
Dr. William S. Rees, Jr. Deputy Under Secretary of Defense (Laboratories and Basic Sciences)	Overview of Relevant Basic Science in DOD
Mr. Bill Linton CEO, Promega	Global View from the Biotech Industry
July 22, 2008	
Dr. Mark M. Little, Senior Vice President and Director, GE Global Research	Discussion on GE Corporate Strategies
July 23, 2008	
Mr. Gregory D. Gordon National Ground Intelligence Center Mr. Paul Parmiter, IMC Dr. Dewey Murdick National Ground Intelligence Center	Discussion on TechWatch
Transition and Fielding Panel	
May 20, 2008	
Mr. Damon Walsh Executive Vice President, Force Protection industries, Inc.	Mine Resistant Ambush Protected (MRAP) Industry Perspective

NAME	TOPIC
Mr. Paul Mann Program Manager MRAP Mr. Barry Dillon Executive Director, MARCORSYSCOM Mr. Will Randolph Assistant Commander for Contracts	MRAP Government Perspective
June 11, 2008	
BG Fox, J8 Office	Joint Urgent Operational Needs Statement, Joint Rapid Acquisition Cell
Dr. Edward Turano Director, Nuclear Technologies Directorate	DOD Research and Development to Counter the Threat from Lost, Stolen and Improvised Nuclear Weapons
June 26, 2008	
Dr. Lin Wells National Defense University	Trends and Shocks
Ms. Kathleen Harger Assistant Deputy Under Secretary of Defense for Innovation and Technology Transition	USD (AT&L) Strategic Initiative on Innovation and Technology Transition
LTC Nick Wager, JDI	Weapons of Mass Destruction/Terrorism
Gen (R) Montgomery Meigs	JIEDDO and WWI Subs
July 23, 2008	
Col. Bishop Director Rapid Equipping Force Mr. Gerald Ferguson Deputy Director, U.S. Army Rapid Equipping Force	Rapid Equipping Force (REF)
Dr. Alok Das Director, Air Force Research Lab, Core Process 3	Air Force Research Lab Core Processes 3
Dr. Leo Christodoulou Defense Sciences Office, Defense Advanced Research Projects Agency	WASP & HARDWIRE
Mr. Mike Knollman Assistant Deputy Under Secretary of Defense for Joint & Coalition Operations Support	Joint and Coalition Operations Support

Glossary

CAWRO	Capability Assessment, Warning, and Response Office
COCOM	combatant commands
DARPA	Defense Advanced Research Projects Agency
DNI	Director of National Intelligence
DOD	Department of Defense
DOTMLPF	doctrine, organization, training, material, leadership and education, personnel, and facilities
DSB	Defense Science Board
DSTL	Defense Science and Technology Laboratory (U.K.)
GPS	Global Positioning System
GWOT	global war on terror
IC	intelligence community
IED	improvised explosive device
I&W	indications and warning
JCS	Joint Chiefs of Staff
JIEDDO	Joint Improvised Explosive Device Defeat Organization
KMT	Kuomintang
KPP	key performance parameters
MILSTAR	Military Strategic and Tactical Relay (Satellite)
MRAP	Mine Resistant Ambush Protected (Vehicle)
NASA	National Aeronautics and Space Administration
NNSA	National Nuclear Security Administration
NRO	National Reconnaissance Office
OECD	Organization for Economic Cooperation and Development
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OPNAV	Office of the Chief of Naval Operations
OSD	Office of the Secretary of Defense
PNT	positioning, navigation, and timing
RAIDRS	Rapid Attack Identification Detection and Reporting System
RCFO	Rapid Capability Fielding Office
R&D	research & development
SATCOM	satellite communication
SBIRS	Space Based Infrared System
SECDEF	Secretary of Defense
TRADOC	U.S. Army Training and Doctrine Command
TTP	tactics, techniques, and procedures
USD (AT&L)	Undersecretary of Defense for Acquisition, Technology, and Logistics
USSR	United Soviet Socialist Republic
WMD	weapons of mass destruction
WTO	World Trade Organization